US 20030079043A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2003/0079043 A1

(43) Pub. Date: Apr. 24, 2003

Citation 1

Chang et al.

(54) VPN SERVICE MANAGEMENT SYSTEM AND VPN SERVICE MANAGER AND VPN SERVICE AGENT COMPRISING SAME

(76) Inventors: Ta-Wei Chang, Kawasaki (JP); Toshimasa Arai, Kawasaki (JP); Yasuko Onodera, Kawasaki (JP); Hiroaki Abe, Kawasaki (JP)

Correspondence Address:
KATTEN MUCHIN ZAVIS ROSENMAN
575 MADISON AVENUE
NEW YORK, NY 10022-2585 (US)

(21) Appl. No.: 10/117,716

(22) Filed: Apr. 5, 2002

(30) Foreign Application Priority Data

Oct. 18, 2001 (JP) 2001-320913

Publication Classification

(51) Int. Cl.[7] G06F 15/16; G06F 15/173

(52) U.S. Cl. 709/249; 709/223

(57) ABSTRACT

A VPN service management system enabling a customer to rapidly and easily change a VPN service condition, that is, a VPN service management system for managing a VPN service for a communication network provided with a customer network and a provider network and having a VPN service manager for managing a VPN service for a provider network and a VPN service agent for managing a VPN service for a customer network. The VPN service manager changes the VPN service condition in real time in accordance with an operation status of the customer network in cooperation with the VPN service agent.

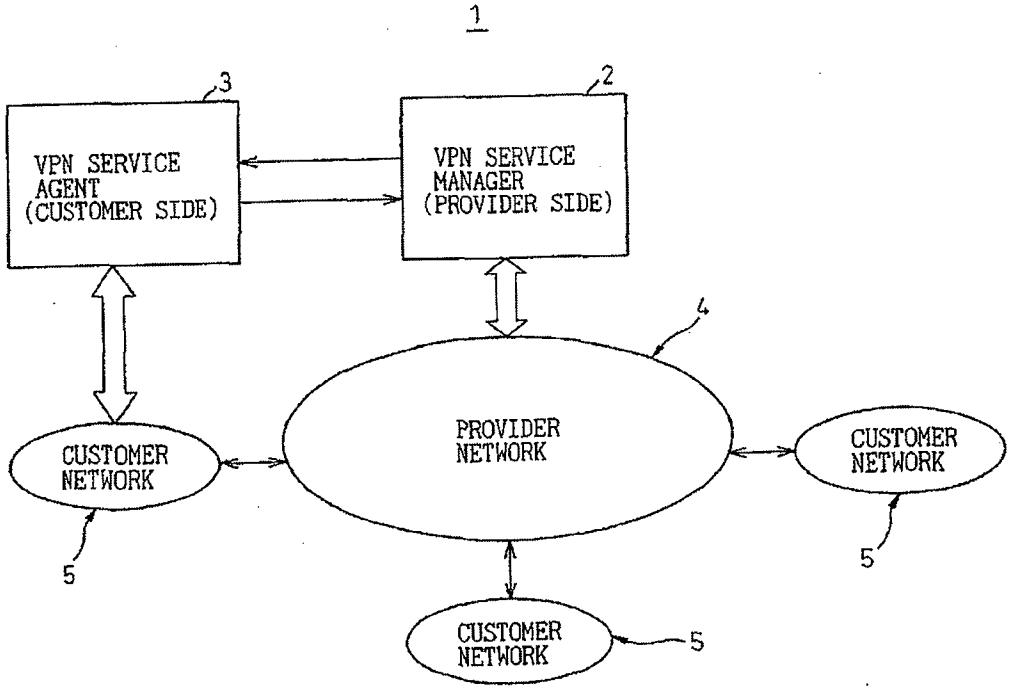


FIG.1

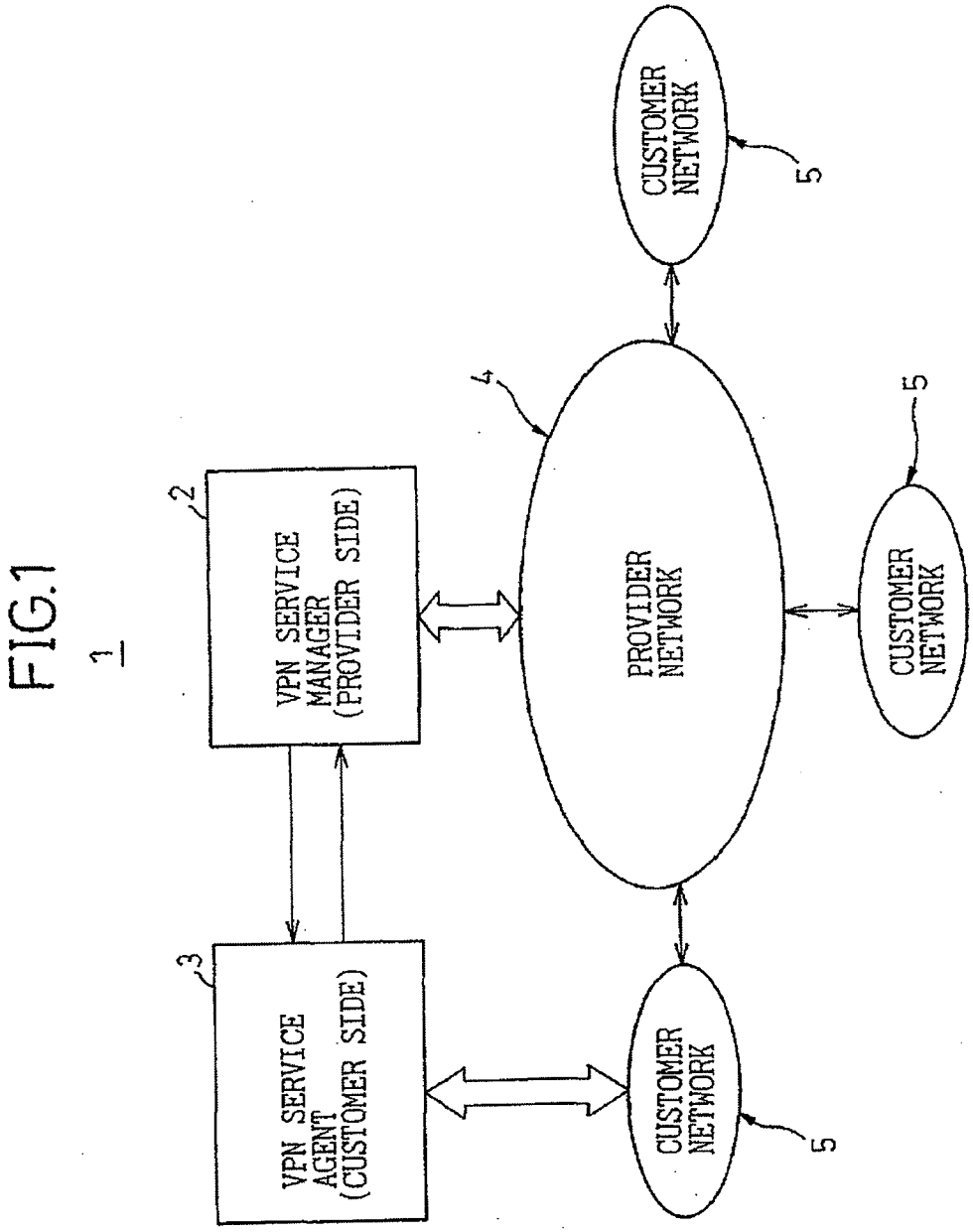

1
2
VPN SERVICE MANAGER (PROVIDER SIDE)
3
VPN SERVICE AGENT (CUSTOMER SIDE)
4
PROVIDER NETWORK
5
CUSTOMER NETWORK
5
CUSTOMER NETWORK
5
CUSTOMER NETWORK

FIG.2

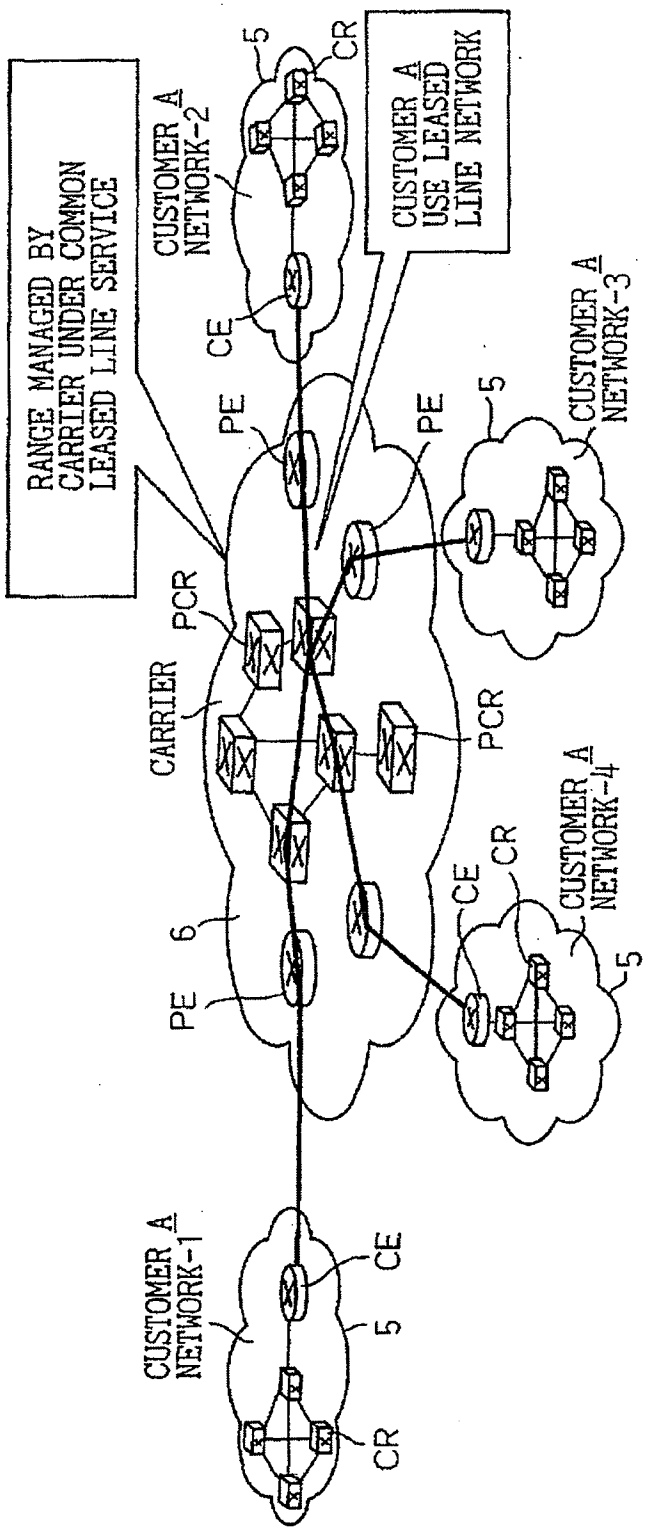

RANGE MANAGED BY CARRIER UNDER COMMON LEASED LINE SERVICE
CUSTOMER A USE LEASED LINE NETWORK
CUSTOMER A NETWORK-1
CUSTOMER A NETWORK-2
CUSTOMER A NETWORK-3
CUSTOMER A NETWORK-4
CARRIER
PE
PCR
CE
CR
5
6

FIG.3

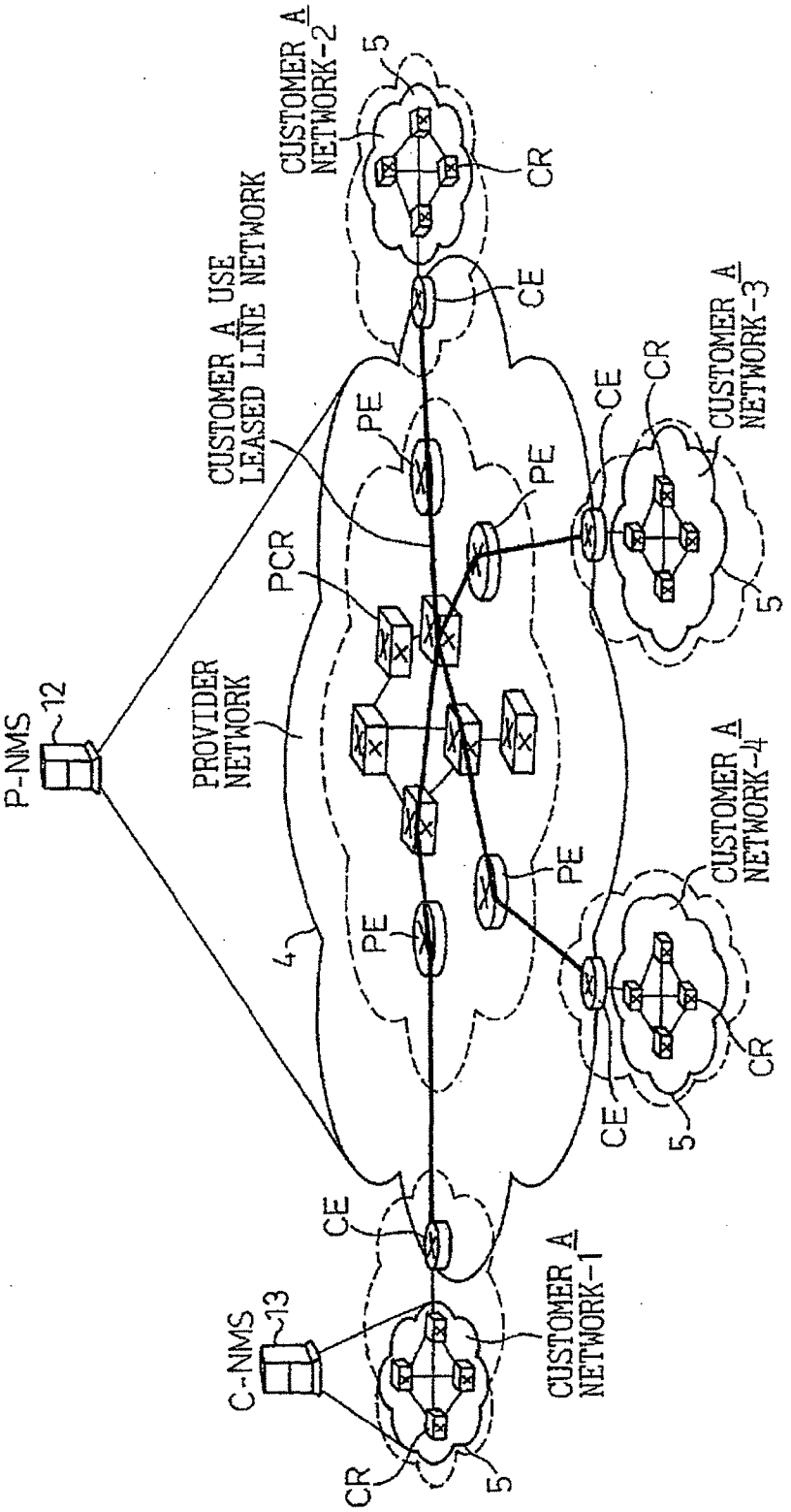

P-NMS
12
C-NMS
13
PROVIDER NETWORK
4
CUSTOMER A USE LEASED LINE NETWORK
PCR
PE
CE
CR
5
CUSTOMER A NETWORK-1
CUSTOMER A NETWORK-2
CUSTOMER A NETWORK-3
CUSTOMER A NETWORK-4

FIG.4

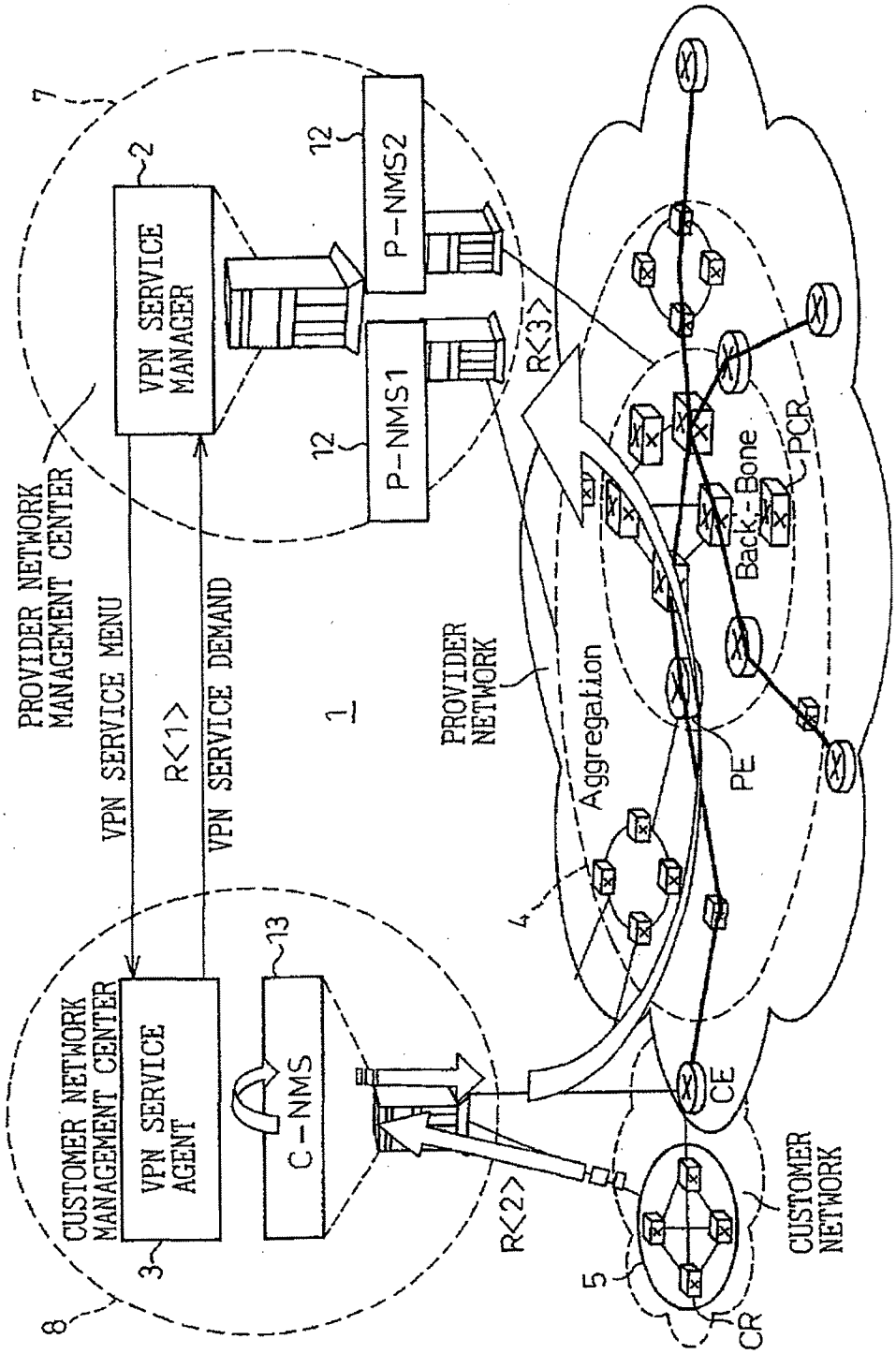

PROVIDER NETWORK MANAGEMENT CENTER
VPN SERVICE MANAGER
P-NMS2
P-NMS1
VPN SERVICE MENU
R<1>
VPN SERVICE DEMAND
1
PROVIDER NETWORK
R<3>
Aggregation
Back-Bone
PCR
PE
CUSTOMER NETWORK MANAGEMENT CENTER
VPN SERVICE AGENT
C-NMS
R<2>
CE
CUSTOMER NETWORK
CR
2
12
12
7
13
3
8
4
5
1

FIG.5

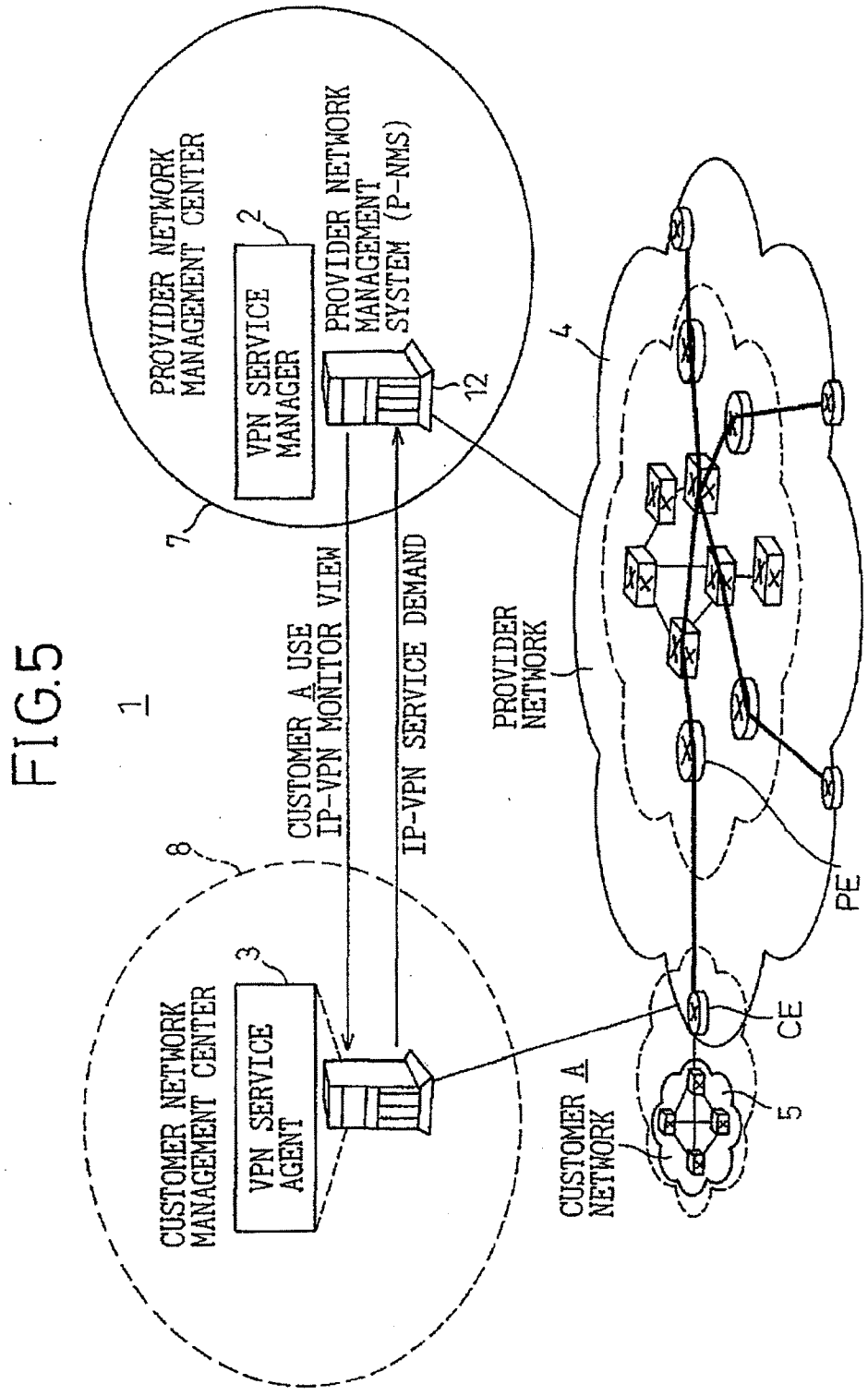

1
PROVIDER NETWORK MANAGEMENT CENTER
2
VPN SERVICE MANAGER
PROVIDER NETWORK MANAGEMENT SYSTEM (P-NMS)
12
7
4
CUSTOMER A USE IP-VPN MONITOR VIEW
IP-VPN SERVICE DEMAND
PROVIDER NETWORK
8
CUSTOMER NETWORK MANAGEMENT CENTER
3
VPN SERVICE AGENT
PE
CE
5
CUSTOMER A NETWORK

FIG.6

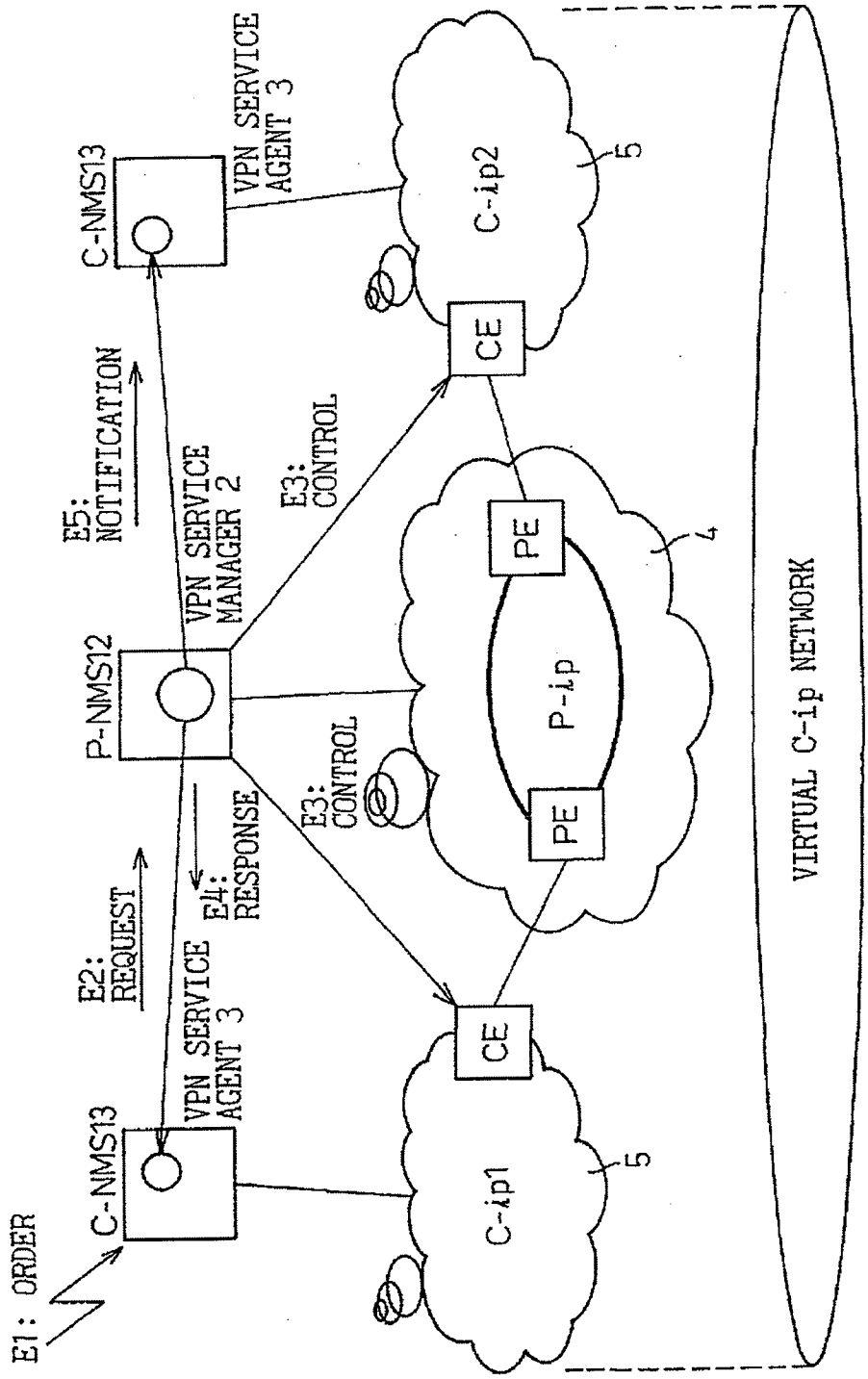

E1: ORDER
C-NMS13
VPN SERVICE AGENT 3
E2: REQUEST
E4: RESPONSE
P-NMS12
VPN SERVICE MANAGER 2
E5: NOTIFICATION
E3: CONTROL
E3: CONTROL
C-NMS13
VPN SERVICE AGENT 3
C-ip1
C-ip2
CE
CE
PE
PE
P-ip
4
5
5
VIRTUAL C-ip NETWORK

FIG.7

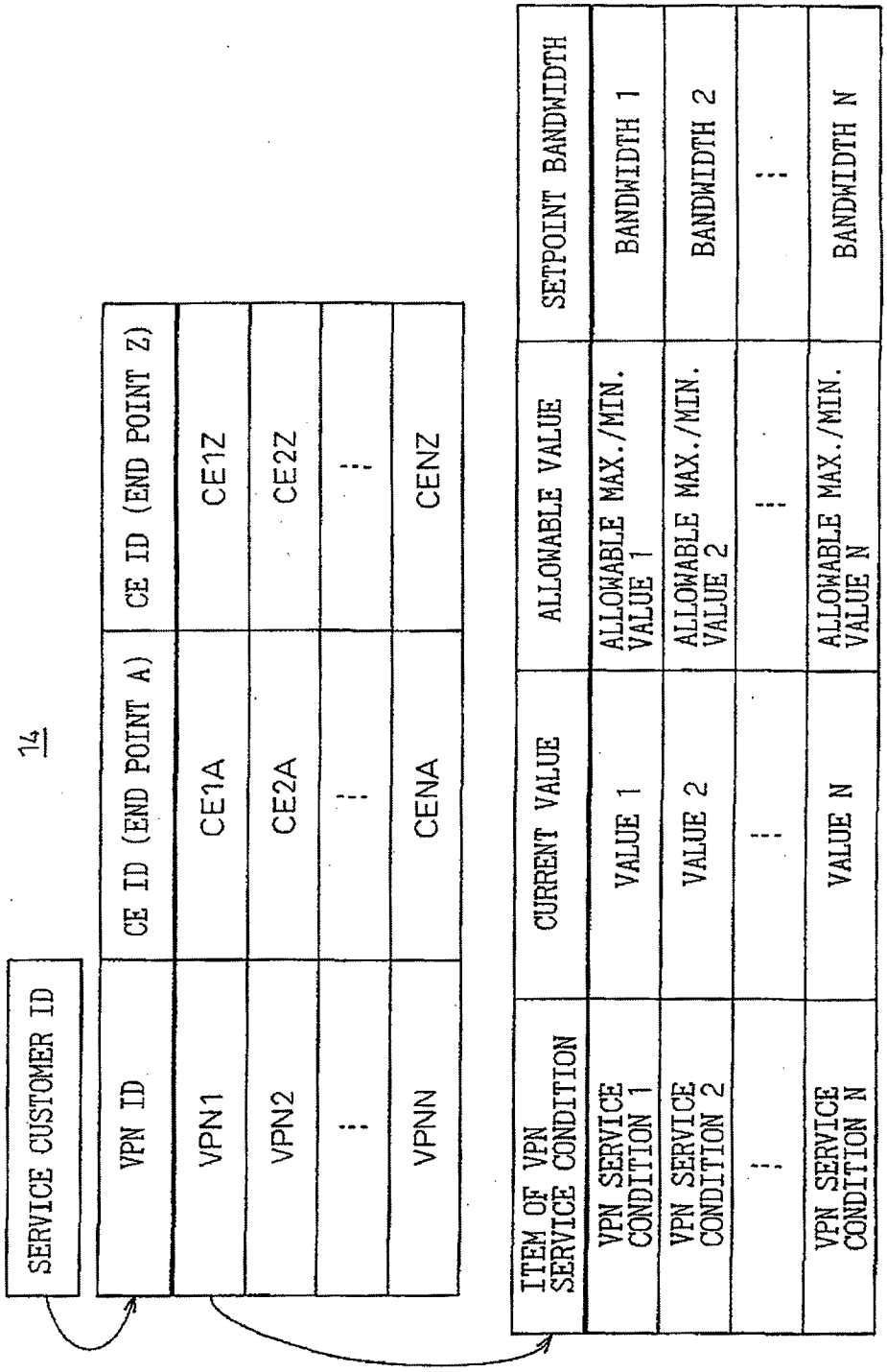

14
SERVICE CUSTOMER ID
VPN ID
CE ID (END POINT A)
CE ID (END POINT Z)
VPN1
CE1A
CE1Z
VPN2
CE2A
CE2Z
VPNN
CENA
CENZ
ITEM OF VPN SERVICE CONDITION
CURRENT VALUE
ALLOWABLE VALUE
SETPOINT BANDWIDTH
VPN SERVICE CONDITION 1
VALUE 1
ALLOWABLE MAX./MIN. VALUE 1
BANDWIDTH 1
VPN SERVICE CONDITION 2
VALUE 2
ALLOWABLE MAX./MIN. VALUE 2
BANDWIDTH 2
VPN SERVICE CONDITION N
VALUE N
ALLOWABLE MAX./MIN. VALUE N
BANDWIDTH N

FIG.8

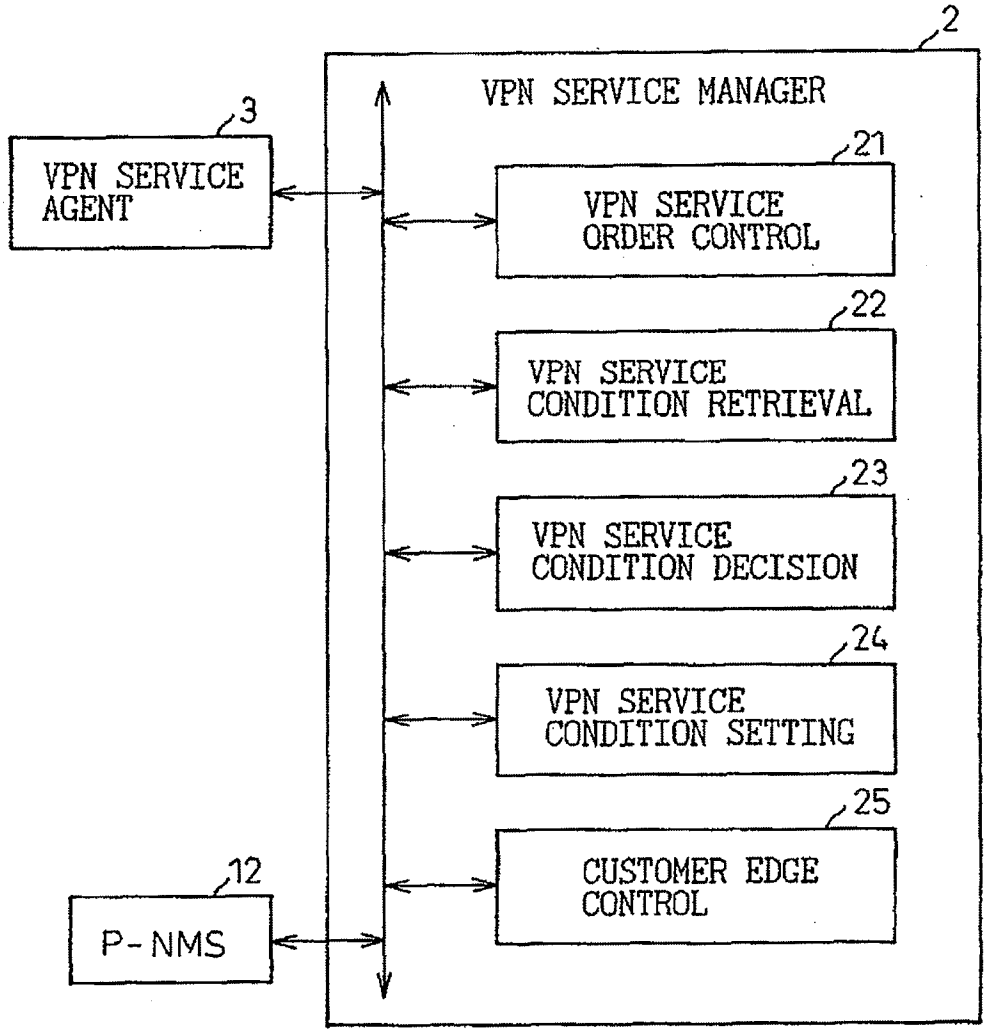

2
VPN SERVICE MANAGER
3
VPN SERVICE AGENT
21
VPN SERVICE ORDER CONTROL
22
VPN SERVICE CONDITION RETRIEVAL
23
VPN SERVICE CONDITION DECISION
24
VPN SERVICE CONDITION SETTING
25
CUSTOMER EDGE CONTROL
12
P-NMS

FIG.9

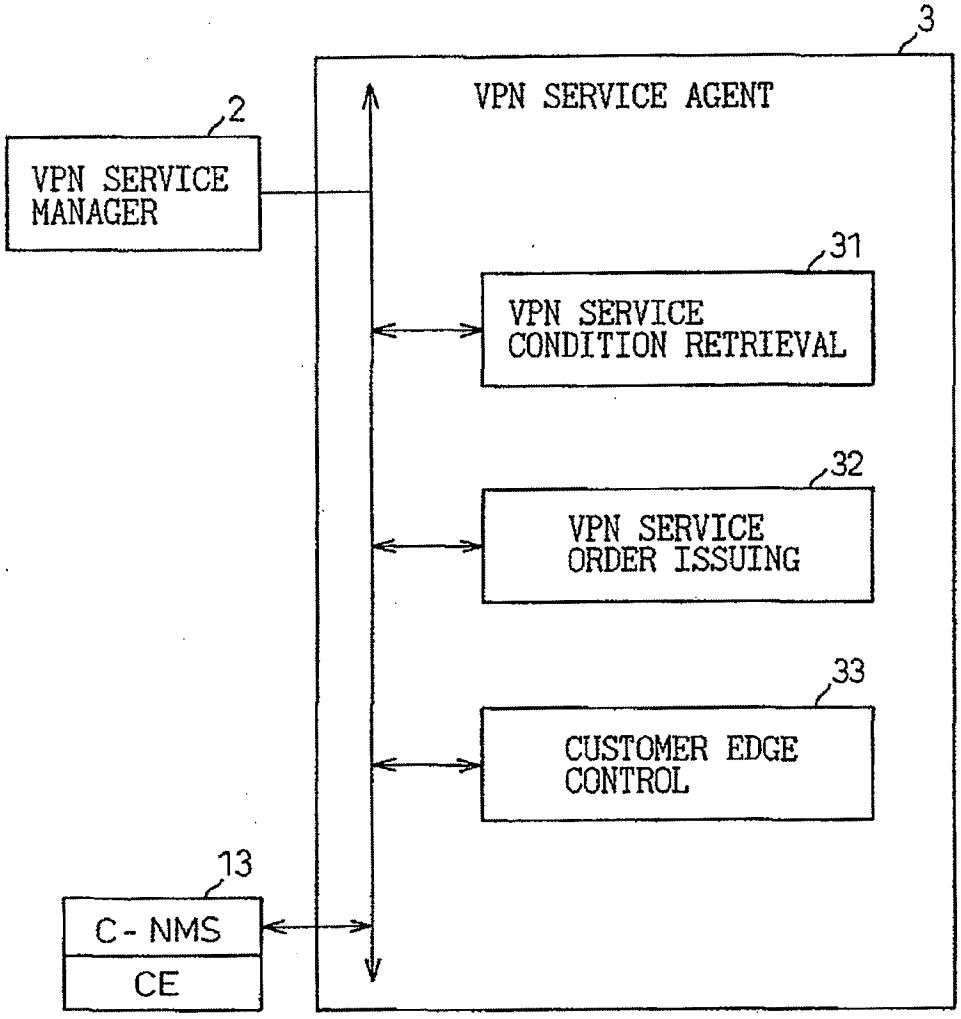

3
VPN SERVICE AGENT
2
VPN SERVICE MANAGER
31
VPN SERVICE CONDITION RETRIEVAL
32
VPN SERVICE ORDER ISSUING
33
CUSTOMER EDGE CONTROL
13
C - NMS
CE

FIG.10

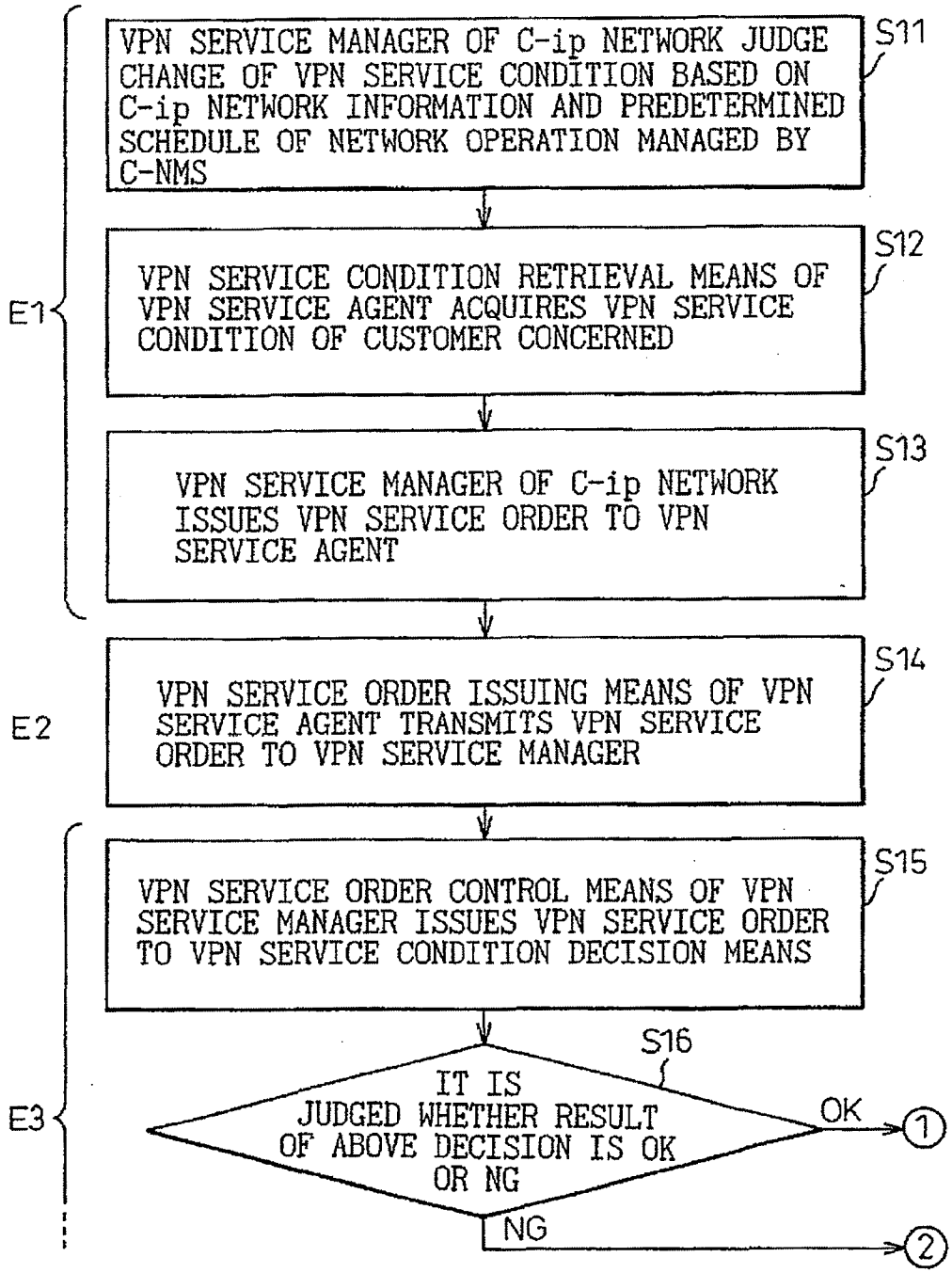

VPN SERVICE MANAGER OF C-ip NETWORK JUDGE CHANGE OF VPN SERVICE CONDITION BASED ON C-ip NETWORK INFORMATION AND PREDETERMINED SCHEDULE OF NETWORK OPERATION MANAGED BY C-NMS
S11
VPN SERVICE CONDITION RETRIEVAL MEANS OF VPN SERVICE AGENT ACQUIRES VPN SERVICE CONDITION OF CUSTOMER CONCERNED
S12
E1
VPN SERVICE MANAGER OF C-ip NETWORK ISSUES VPN SERVICE ORDER TO VPN SERVICE AGENT
S13
VPN SERVICE ORDER ISSUING MEANS OF VPN SERVICE AGENT TRANSMITS VPN SERVICE ORDER TO VPN SERVICE MANAGER
S14
E2
VPN SERVICE ORDER CONTROL MEANS OF VPN SERVICE MANAGER ISSUES VPN SERVICE ORDER TO VPN SERVICE CONDITION DECISION MEANS
S15
S16
IT IS JUDGED WHETHER RESULT OF ABOVE DECISION IS OK OR NG
OK
NG
E3
1
2

FIG.11

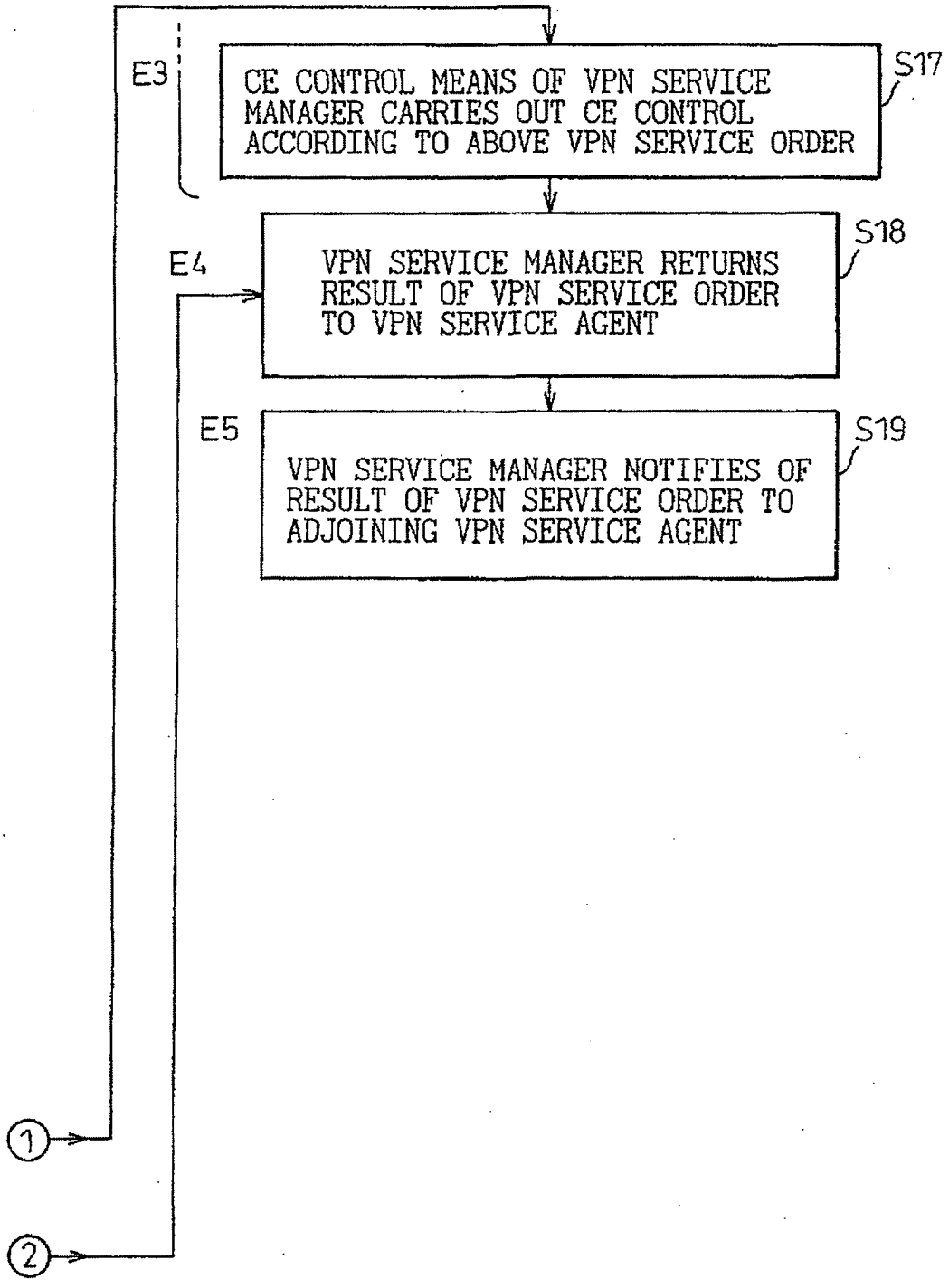

E3
CE CONTROL MEANS OF VPN SERVICE MANAGER CARRIES OUT CE CONTROL ACCORDING TO ABOVE VPN SERVICE ORDER
S17
E4
VPN SERVICE MANAGER RETURNS RESULT OF VPN SERVICE ORDER TO VPN SERVICE AGENT
S18
E5
VPN SERVICE MANAGER NOTIFIES OF RESULT OF VPN SERVICE ORDER TO ADJOINING VPN SERVICE AGENT
S19
1
2

FIG.12

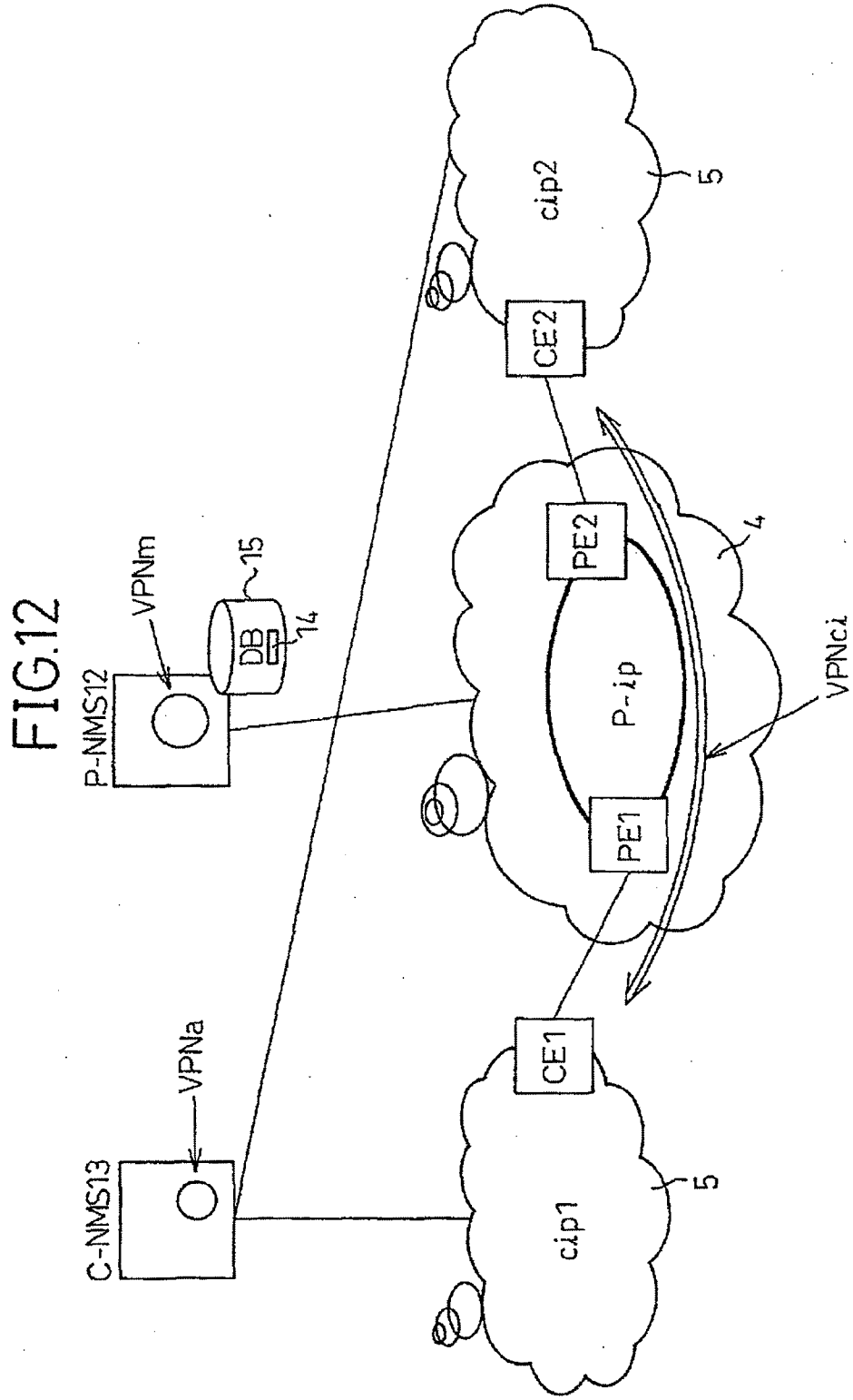

cip2
5
CE2
PE2
4
P-ip
VPNci
PE1
CE1
cip1
5
C-NMS13
VPNa
P-NMS12
VPNm
DB
15
14

FIG.13

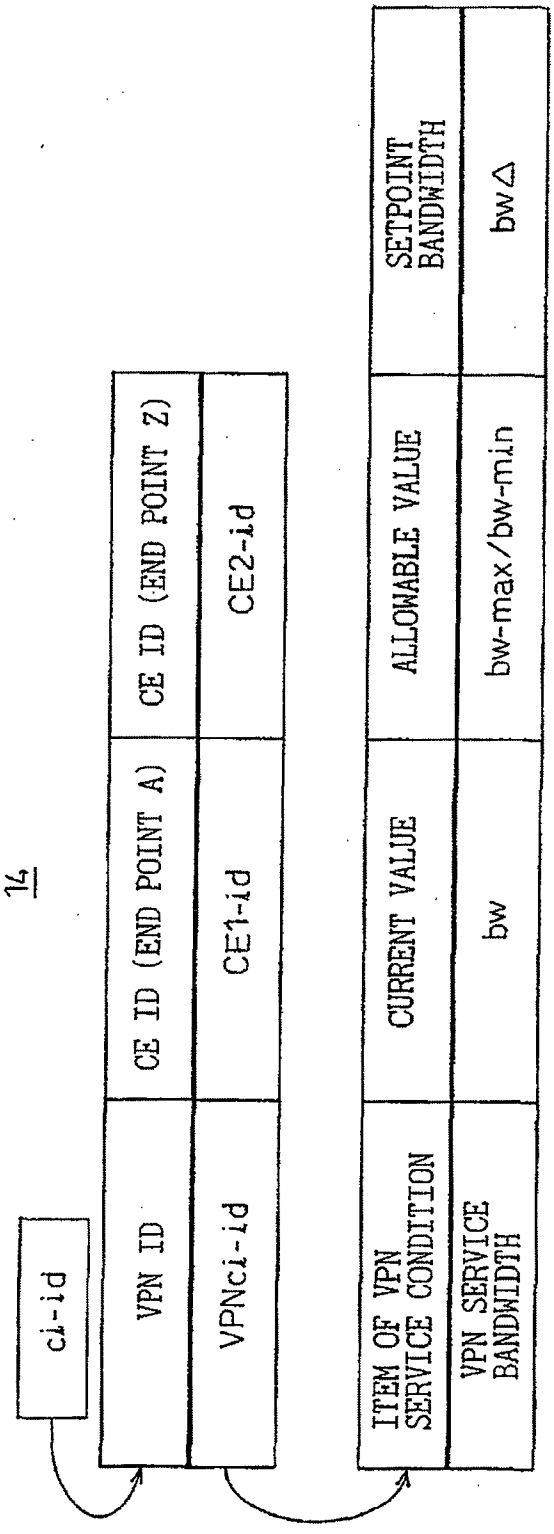

14
ci-id
VPN ID
VPNci-id
CE ID (END POINT A)
CE1-id
CE ID (END POINT Z)
CE2-id
ITEM OF VPN SERVICE CONDITION
VPN SERVICE BANDWIDTH
CURRENT VALUE
bw
ALLOWABLE VALUE
bw-max/bw-min
SETPOINT BANDWIDTH
bw△

FIG.14

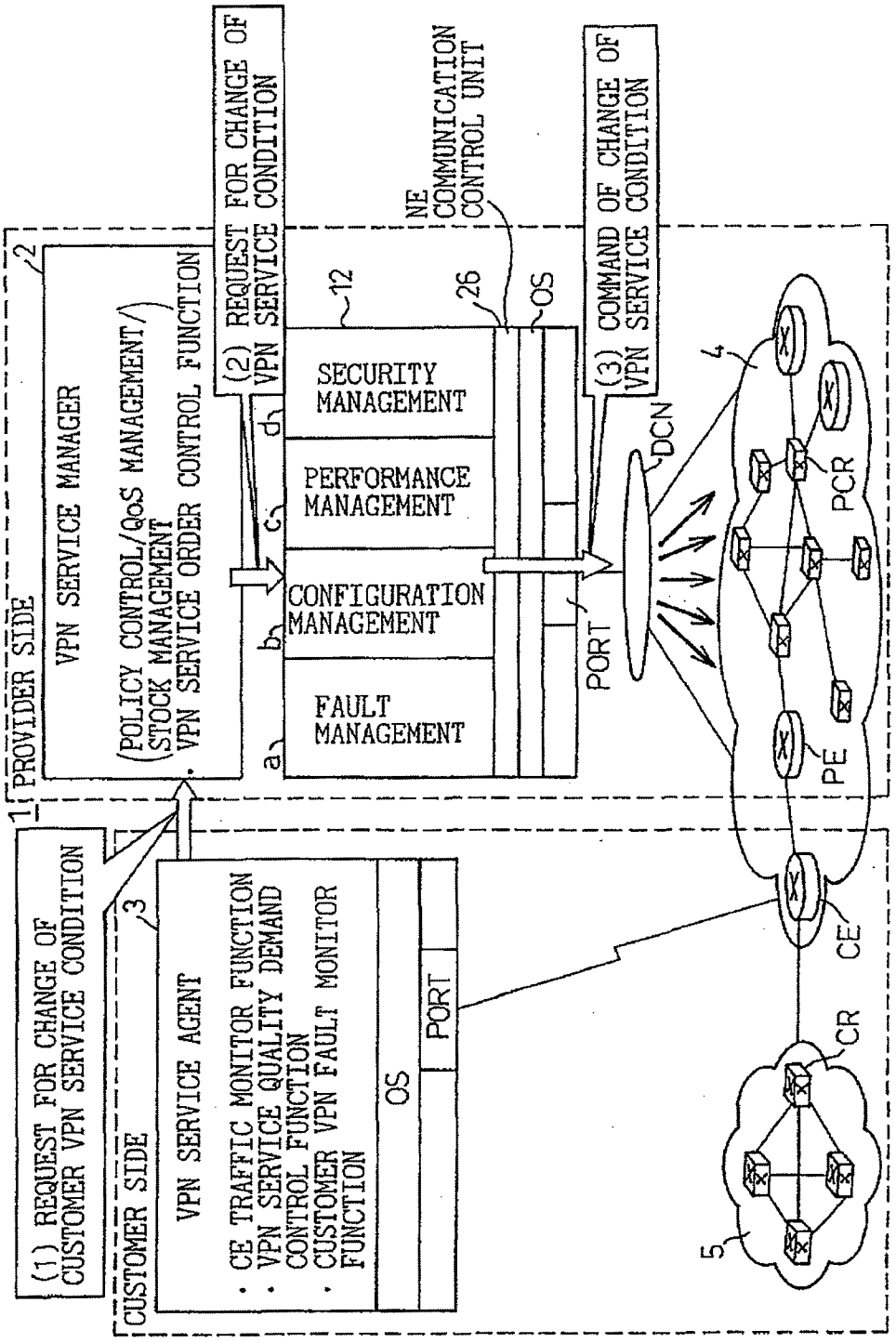

1
PROVIDER SIDE
2
VPN SERVICE MANAGER
(POLICY CONTROL/QoS MANAGEMENT)
(STOCK MANAGEMENT
· VPN SERVICE ORDER CONTROL FUNCTION
(2) REQUEST FOR CHANGE OF VPN SERVICE CONDITION
12
SECURITY MANAGEMENT
PERFORMANCE MANAGEMENT
CONFIGURATION MANAGEMENT
FAULT MANAGEMENT
a
b
c
d
NE COMMUNICATION CONTROL UNIT
26
OS
PORT
(3) COMMAND OF CHANGE OF VPN SERVICE CONDITION
DCN
4
PCR
PE
CE
CR
5
(1) REQUEST FOR CHANGE OF CUSTOMER VPN SERVICE CONDITION
CUSTOMER SIDE
3
VPN SERVICE AGENT
· CE TRAFFIC MONITOR FUNCTION
· VPN SERVICE QUALITY DEMAND CONTROL FUNCTION
· CUSTOMER VPN FAULT MONITOR FUNCTION
OS
PORT

FIG.15

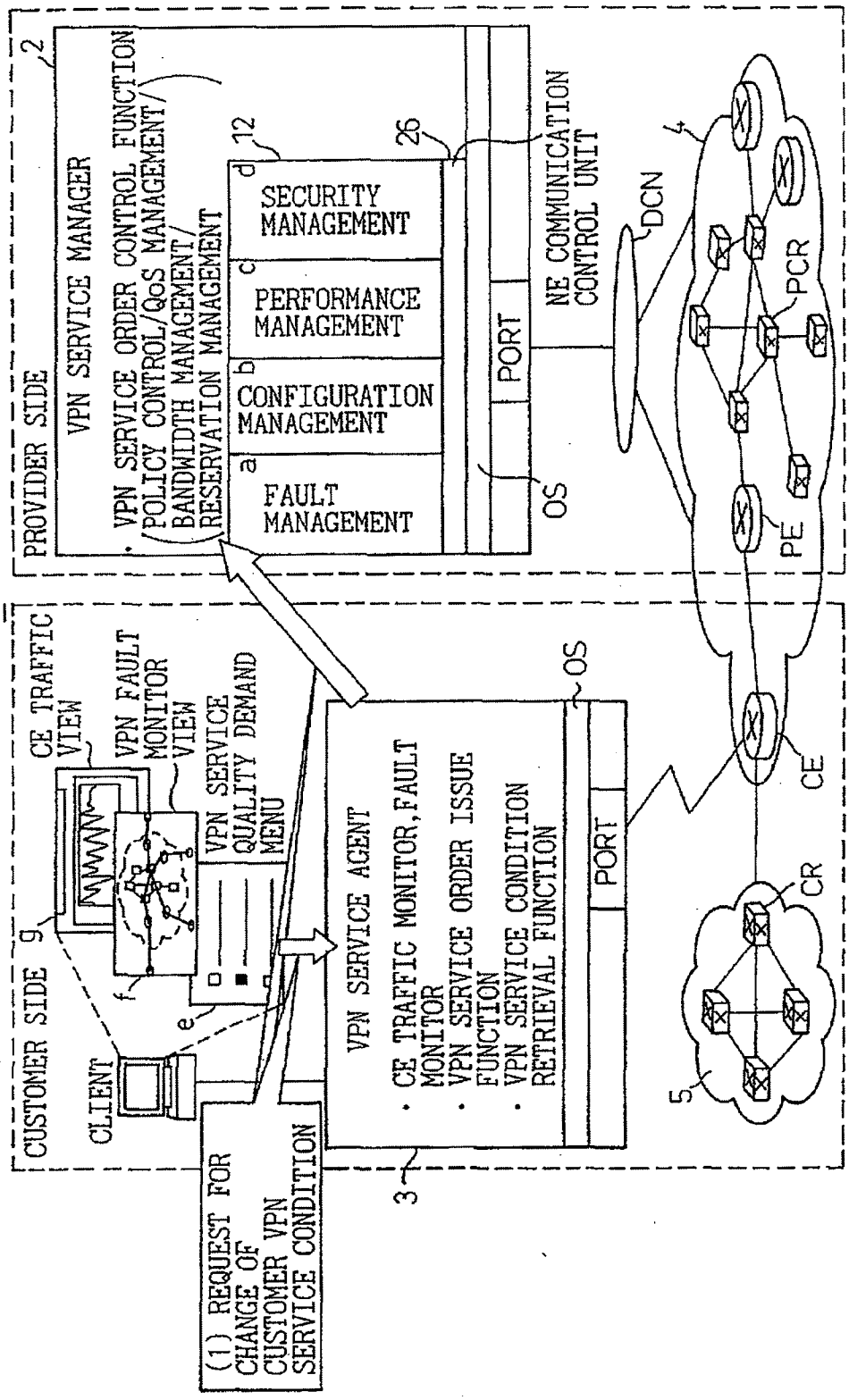

PROVIDER SIDE
2
VPN SERVICE MANAGER
· VPN SERVICE ORDER CONTROL FUNCTION (POLICY CONTROL/QoS MANAGEMENT/ BANDWIDTH MANAGEMENT/ RESERVATION MANAGEMENT)
a FAULT MANAGEMENT
b CONFIGURATION MANAGEMENT
c PERFORMANCE MANAGEMENT
d SECURITY MANAGEMENT
12
26
PORT
OS
NE COMMUNICATION CONTROL UNIT
DCN
4
PCR
PE
CE
CR
5
CUSTOMER SIDE
1
CE TRAFFIC VIEW
VPN FAULT MONITOR VIEW
VPN SERVICE QUALITY DEMAND MENU
9
f
e
CLIENT
VPN SERVICE AGENT
· CE TRAFFIC MONITOR, FAULT MONITOR
· VPN SERVICE ORDER ISSUE FUNCTION
· VPN SERVICE CONDITION RETRIEVAL FUNCTION
OS
PORT
3
(1) REQUEST FOR CHANGE OF CUSTOMER VPN SERVICE CONDITION

FIG.16

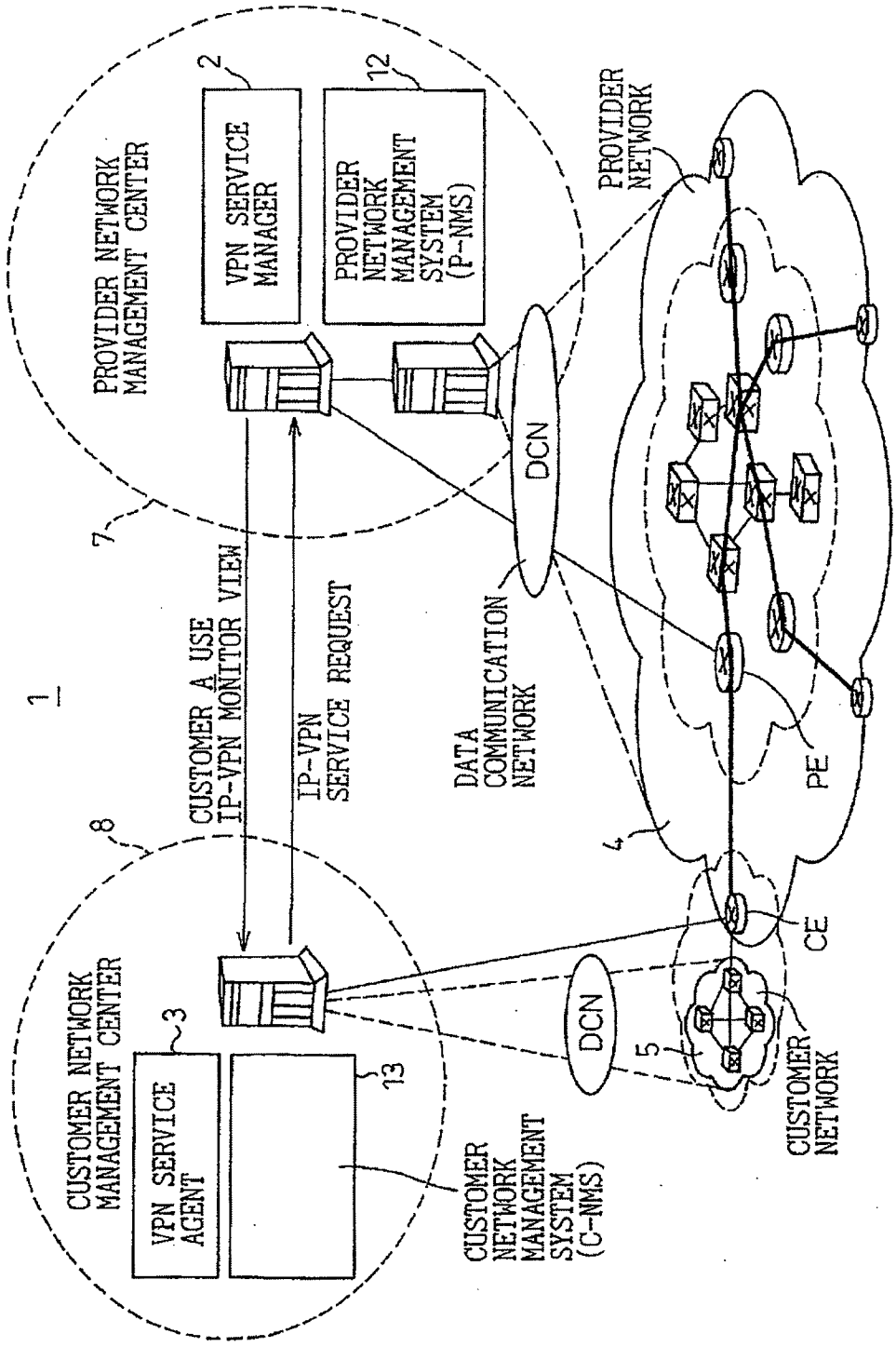

1
PROVIDER NETWORK MANAGEMENT CENTER
2
VPN SERVICE MANAGER
12
PROVIDER NETWORK MANAGEMENT SYSTEM (P-NMS)
7
PROVIDER NETWORK
DCN
DATA COMMUNICATION NETWORK
CUSTOMER A USE IP-VPN MONITOR VIEW
IP-VPN SERVICE REQUEST
8
CUSTOMER NETWORK MANAGEMENT CENTER
3
VPN SERVICE AGENT
13
CUSTOMER NETWORK MANAGEMENT SYSTEM (C-NMS)
DCN
4
PE
CE
5
CUSTOMER NETWORK

FIG.17

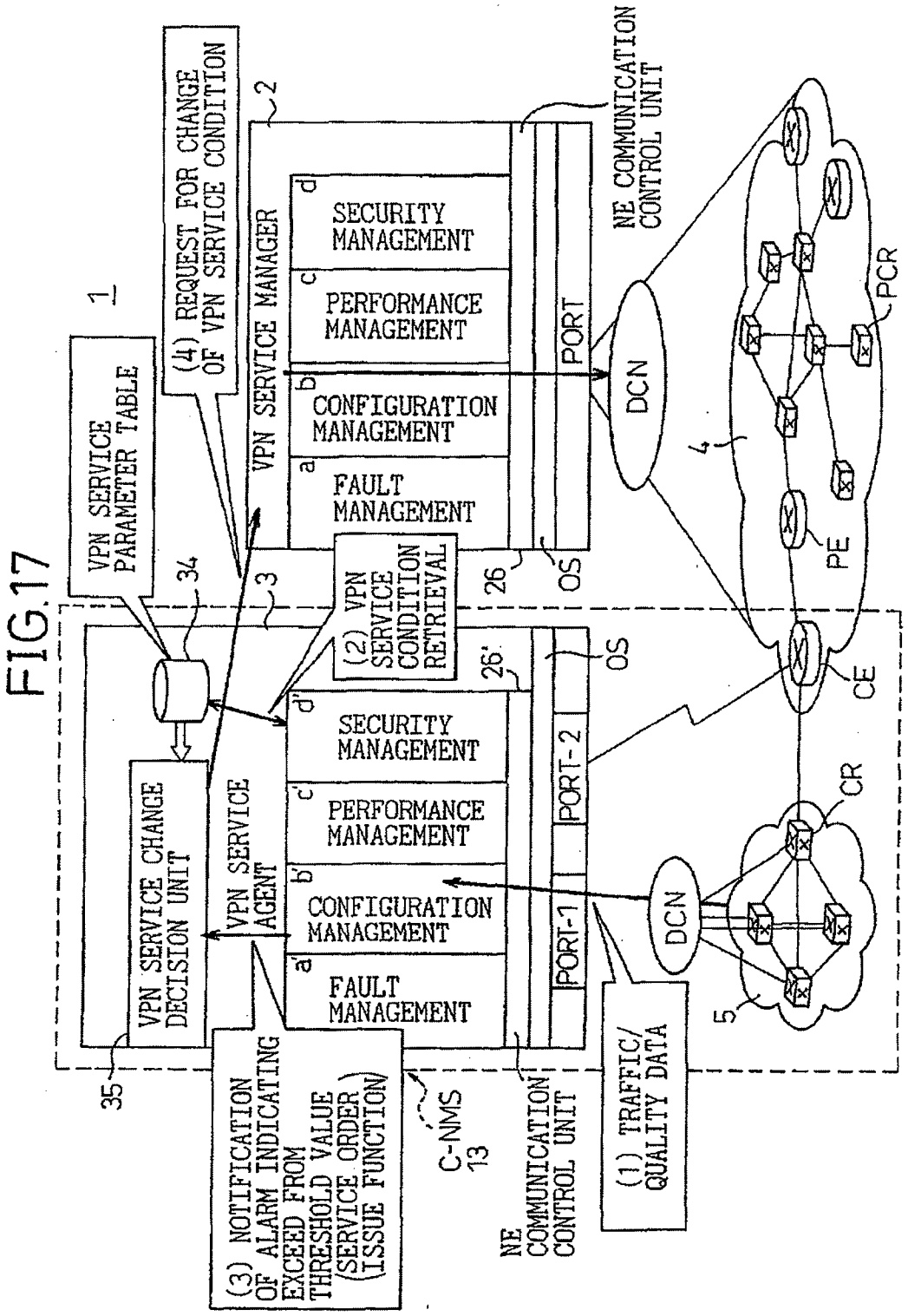

1
VPN SERVICE PARAMETER TABLE
(4) REQUEST FOR CHANGE OF VPN SERVICE CONDITION
2
VPN SERVICE MANAGER
d SECURITY MANAGEMENT
c PERFORMANCE MANAGEMENT
b CONFIGURATION MANAGEMENT
a FAULT MANAGEMENT
NE COMMUNICATION CONTROL UNIT
PORT
DCN
PCR
4
PE
CE
CR
5
34
3
(2) VPN SERVICE CONDITION RETRIEVAL
26
OS
26'
OS
d' SECURITY MANAGEMENT
c' PERFORMANCE MANAGEMENT
b' CONFIGURATION MANAGEMENT
a' FAULT MANAGEMENT
PORT-2
PORT-1
DCN
VPN SERVICE CHANGE DECISION UNIT
VPN SERVICE AGENT
35
(3) NOTIFICATION OF ALARM INDICATING EXCEED FROM THRESHOLD VALUE (SERVICE ORDER) (ISSUE FUNCTION)
C-NMS 13
NE COMMUNICATION CONTROL UNIT
(1) TRAFFIC/ QUALITY DATA

FIG.18

34

ITEM OF VPN SERVICE CONDITION	CURRENT VALUE	ALLOWABLE VALUE	SETPOINT BANDWIDTH
VPN SERVICE CONDITION 1	VALUE 1	ALLOWABLE MAX./MIN. 1	BANDWIDTH 1
VPN SERVICE CONDITION 2	VALUE 2	ALLOWABLE MAX./MIN. 2	BANDWIDTH 2
⋮	⋮	⋮	⋮
VPN SERVICE CONDITION N	VALUE N	ALLOWABLE MAX./MIN. N	BANDWIDTH N

LEVEL	CURRENT VALUE	CHANGED VALUE
LEVEL 1:	BEST EFFORT (BF)	20% UP FROM BF
LEVEL 2:	20% UP	50% UP
LEVEL 3:	50% UP	100% UP

FIG.19

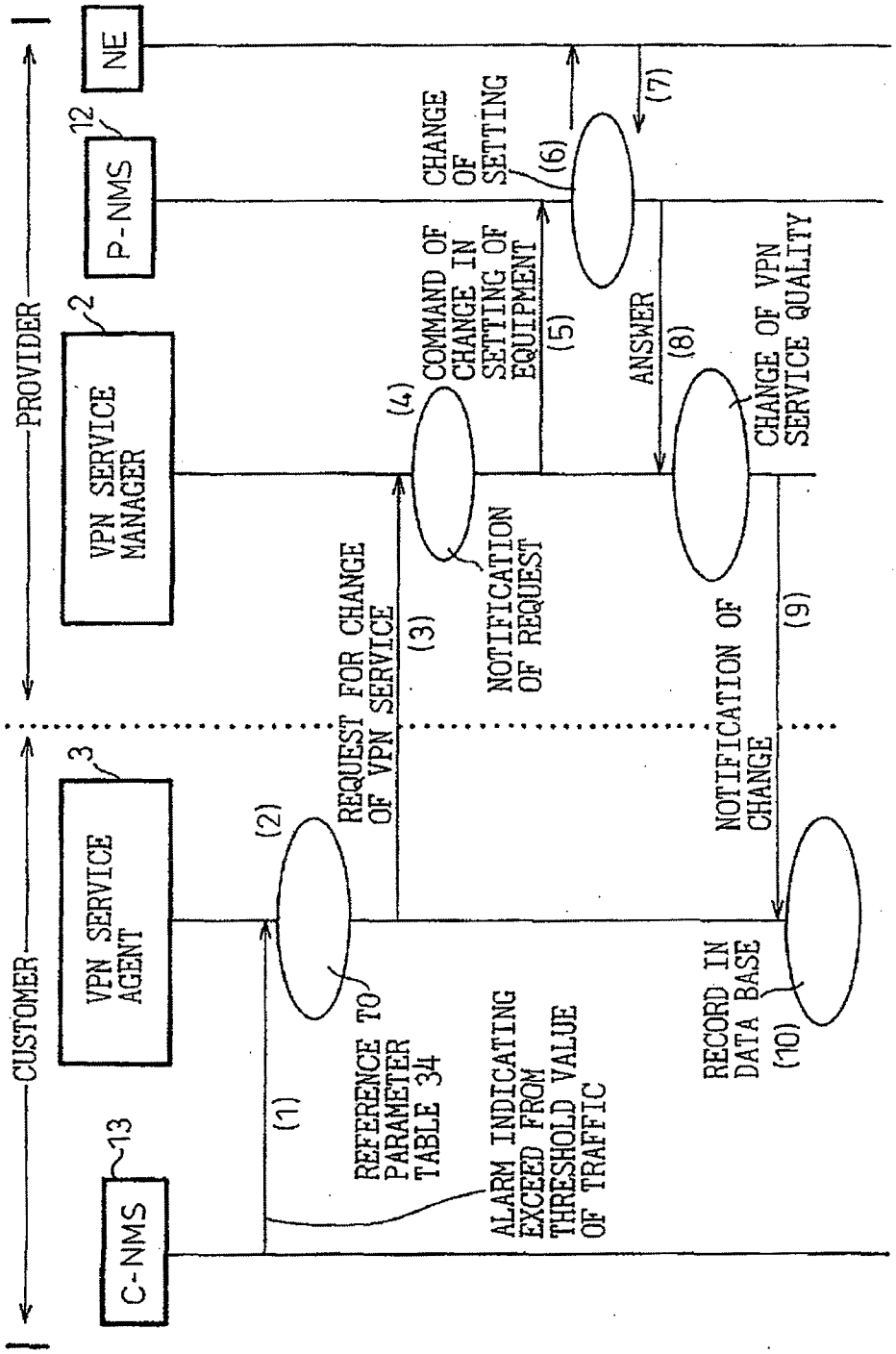

PROVIDER
CUSTOMER
NE
12
P-NMS
2
VPN SERVICE MANAGER
3
VPN SERVICE AGENT
13
C-NMS
(1)
REFERENCE TO PARAMETER TABLE 34
ALARM INDICATING EXCEED FROM THRESHOLD VALUE OF TRAFFIC
(2)
REQUEST FOR CHANGE OF VPN SERVICE
(3)
(4)
COMMAND OF CHANGE IN SETTING OF EQUIPMENT
NOTIFICATION OF REQUEST
(5)
CHANGE OF SETTING
(6)
(7)
ANSWER
(8)
CHANGE OF VPN SERVICE QUALITY
(9)
NOTIFICATION OF CHANGE
RECORD IN DATA BASE
(10)

FIG.20

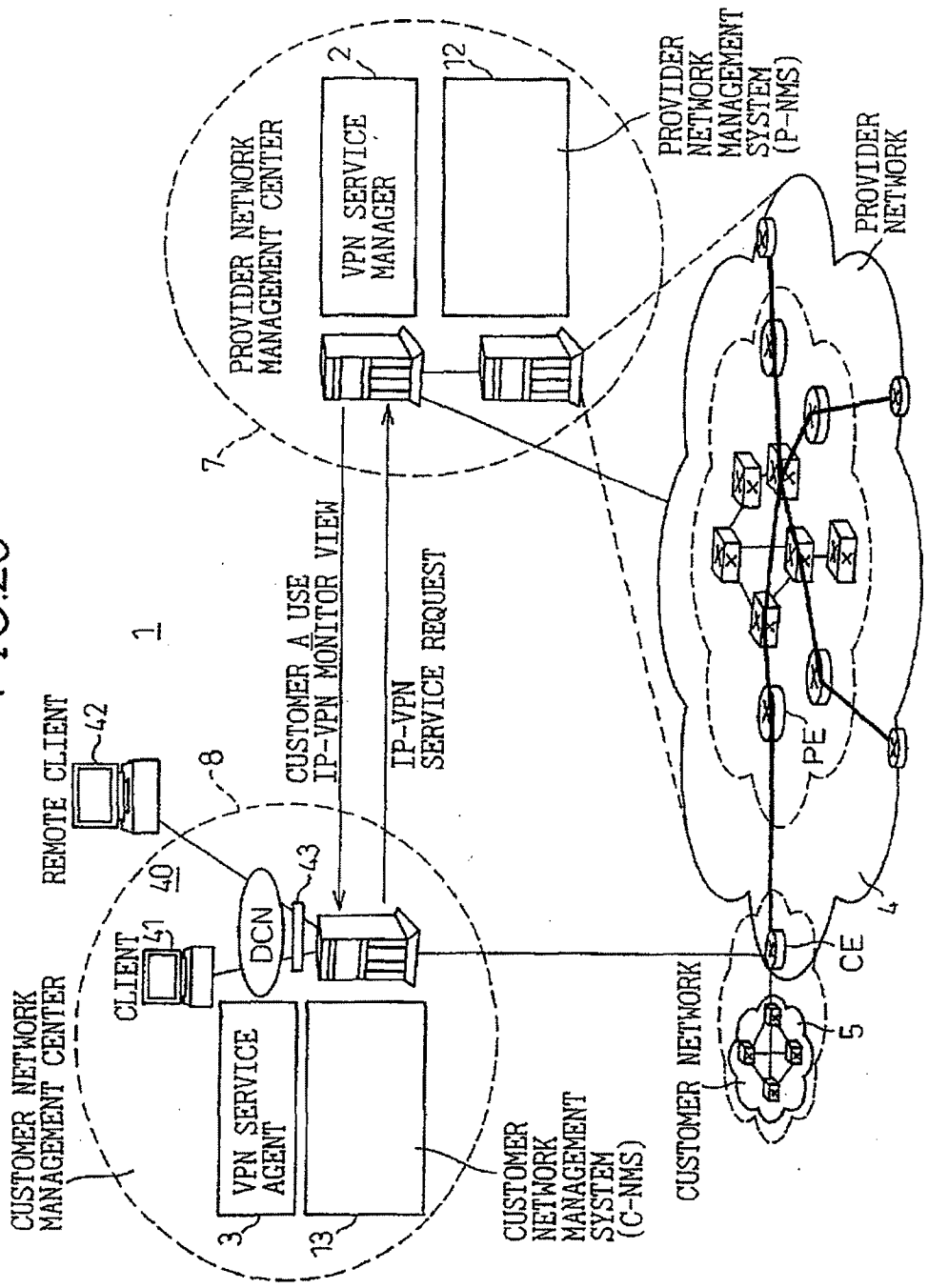

1
PROVIDER NETWORK MANAGEMENT CENTER
VPN SERVICE MANAGER
2
12
7
PROVIDER NETWORK MANAGEMENT SYSTEM (P-NMS)
PROVIDER NETWORK
CUSTOMER A USE IP-VPN MONITOR VIEW
IP-VPN SERVICE REQUEST
REMOTE CLIENT
42
8
40
41
CLIENT
DCN
43
CUSTOMER NETWORK MANAGEMENT CENTER
VPN SERVICE AGENT
3
13
CUSTOMER NETWORK MANAGEMENT SYSTEM (C-NMS)
PE
CE
4
5
CUSTOMER NETWORK

FIG.21

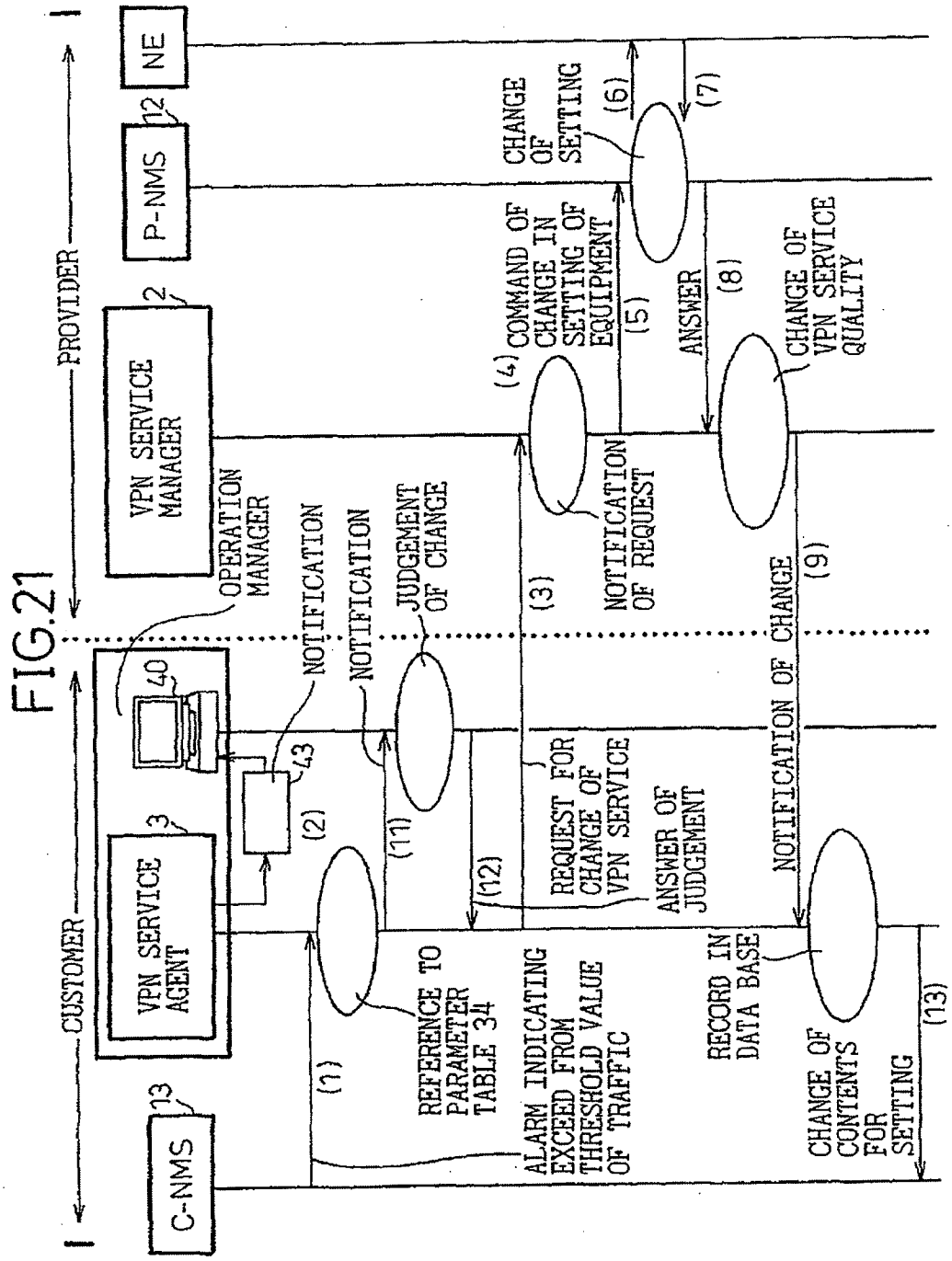

PROVIDER
CUSTOMER
NE
P-NMS
12
VPN SERVICE MANAGER
2
OPERATION MANAGER
40
VPN SERVICE AGENT
3
C-NMS
13
43
NOTIFICATION
NOTIFICATION
JUDGEMENT OF CHANGE
(1)
(2)
(3)
(4) COMMAND OF CHANGE IN SETTING OF EQUIPMENT
(5)
(6) CHANGE OF SETTING
(7)
(8)
(9)
(11)
(12)
(13)
NOTIFICATION OF REQUEST
ANSWER
CHANGE OF VPN SERVICE QUALITY
REQUEST FOR CHANGE OF VPN SERVICE
ANSWER OF JUDGEMENT
NOTIFICATION OF CHANGE
REFERENCE TO PARAMETER TABLE 34
ALARM INDICATING EXCEED FROM THRESHOLD VALUE OF TRAFFIC
RECORD IN DATA BASE
CHANGE OF CONTENTS FOR SETTING

FIG.22

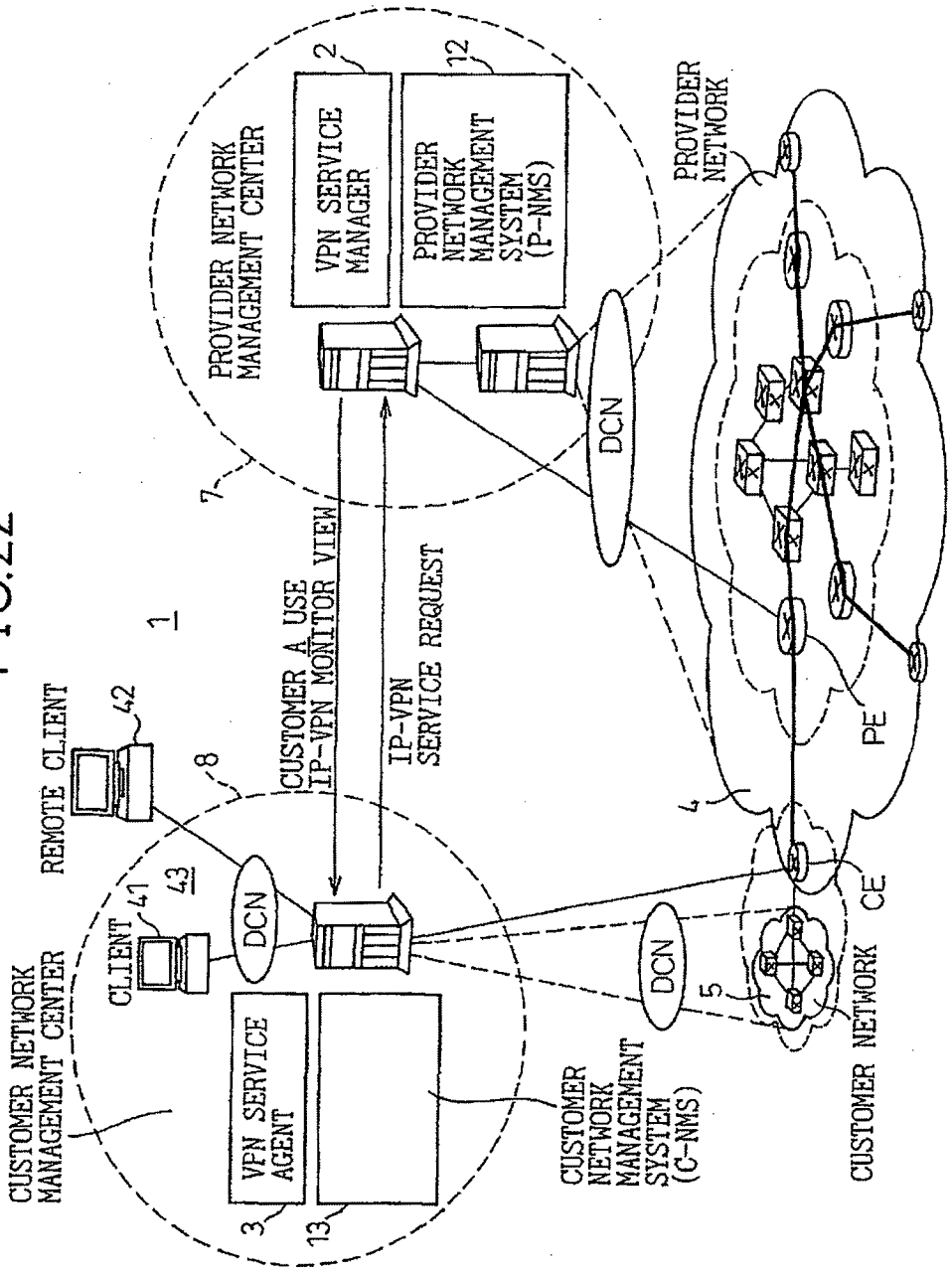

1
PROVIDER NETWORK MANAGEMENT CENTER
VPN SERVICE MANAGER
PROVIDER NETWORK MANAGEMENT SYSTEM (P-NMS)
2
12
7
DCN
PROVIDER NETWORK
PE
4
CUSTOMER A USE IP-VPN MONITOR VIEW
IP-VPN SERVICE REQUEST
REMOTE CLIENT
42
8
CLIENT
41
43
DCN
DCN
5
CE
CUSTOMER NETWORK
CUSTOMER NETWORK MANAGEMENT CENTER
VPN SERVICE AGENT
3
13
CUSTOMER NETWORK MANAGEMENT SYSTEM (C-NMS)

FIG.23

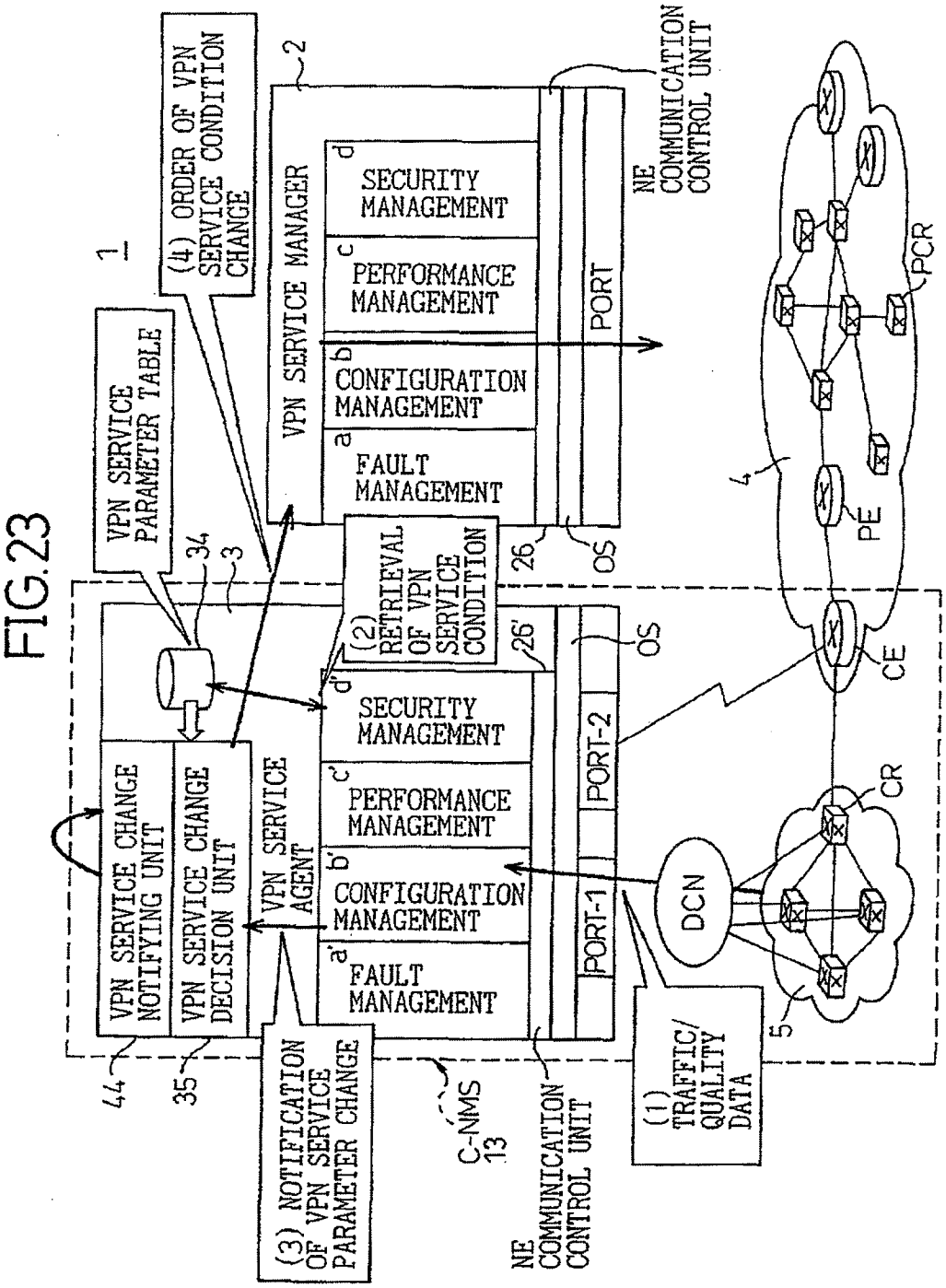

1
(4) ORDER OF VPN SERVICE CONDITION CHANGE
VPN SERVICE PARAMETER TABLE
2
VPN SERVICE MANAGER
d SECURITY MANAGEMENT
c PERFORMANCE MANAGEMENT
b CONFIGURATION MANAGEMENT
a FAULT MANAGEMENT
NE COMMUNICATION CONTROL UNIT
PORT
26
OS
(2) RETRIEVAL OF VPN SERVICE CONDITION
34
3
26'
OS
d' SECURITY MANAGEMENT
c' PERFORMANCE MANAGEMENT
b' CONFIGURATION MANAGEMENT
a' FAULT MANAGEMENT
PORT-2
PORT-1
VPN SERVICE AGENT
VPN SERVICE CHANGE NOTIFYING UNIT
VPN SERVICE CHANGE DECISION UNIT
44
35
(3) NOTIFICATION OF VPN SERVICE PARAMETER CHANGE
C-NMS 13
NE COMMUNICATION CONTROL UNIT
(1) TRAFFIC/ QUALITY DATA
DCN
4
PCR
PE
CE
CR
5

FIG.24

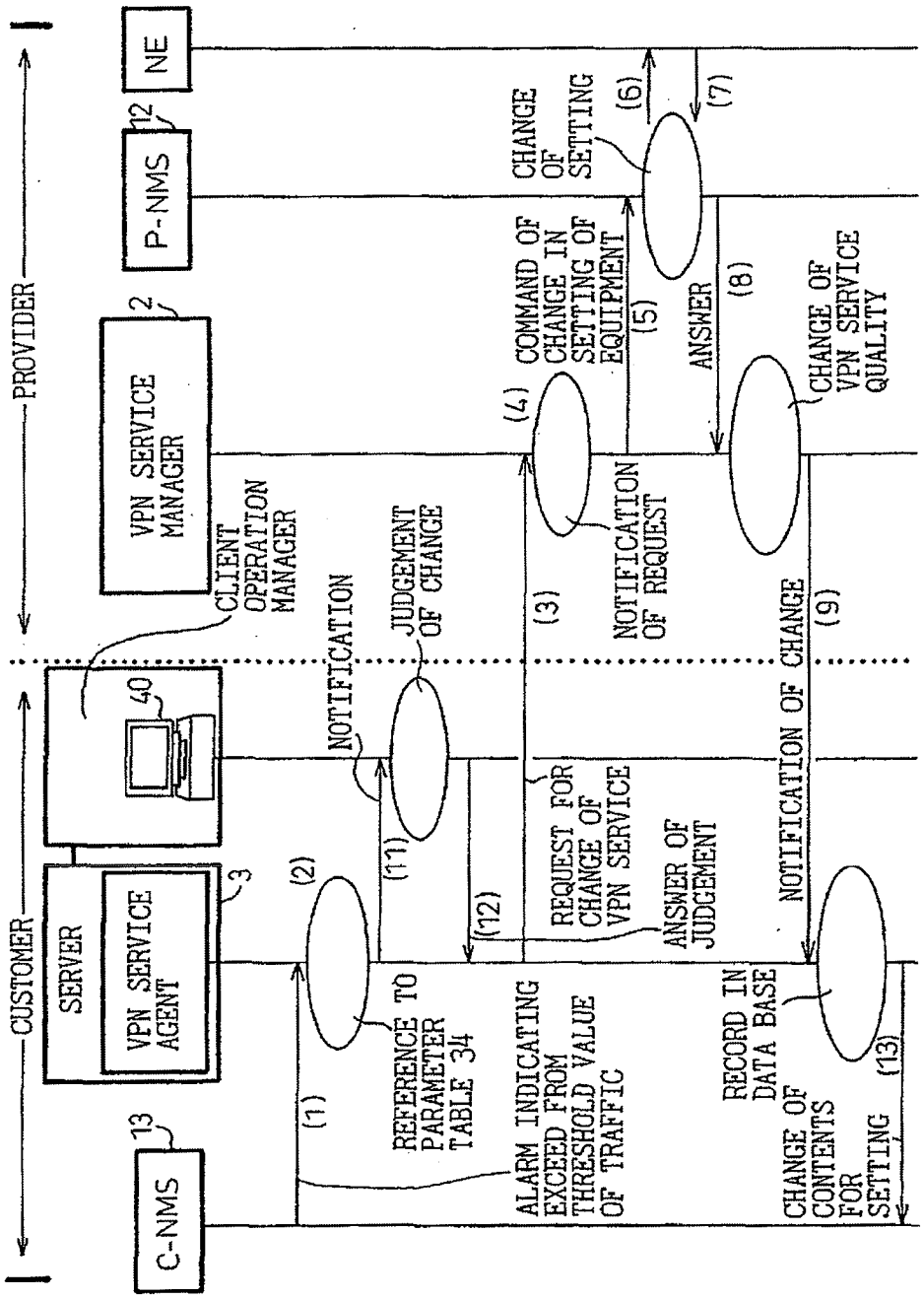

PROVIDER
CUSTOMER
NE
P-NMS
12
VPN SERVICE MANAGER
2
CLIENT OPERATION MANAGER
40
SERVER
VPN SERVICE AGENT
3
C-NMS
13
(1)
ALARM INDICATING EXCEED FROM THRESHOLD VALUE OF TRAFFIC
(2)
REFERENCE TO PARAMETER TABLE 34
NOTIFICATION
(11)
JUDGEMENT OF CHANGE
(12)
(3)
REQUEST FOR CHANGE OF VPN SERVICE
ANSWER OF JUDGEMENT
(4)
COMMAND OF CHANGE IN SETTING OF EQUIPMENT
NOTIFICATION OF REQUEST
(5)
ANSWER
(6)
CHANGE OF SETTING
(7)
(8)
CHANGE OF VPN SERVICE QUALITY
(9)
NOTIFICATION OF CHANGE
RECORD IN DATA BASE
CHANGE OF CONTENTS FOR SETTING
(13)

FIG.25

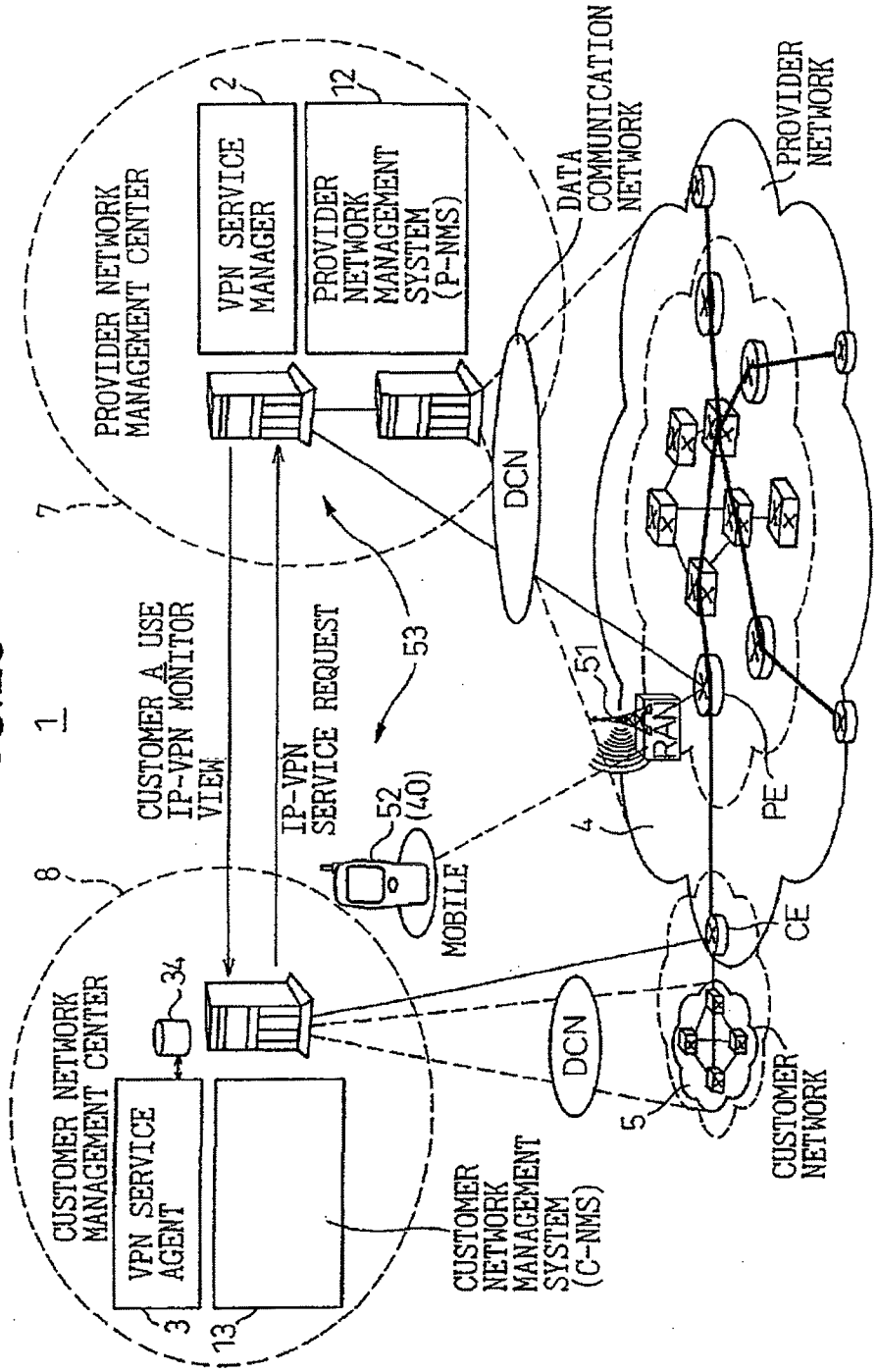

1
PROVIDER NETWORK MANAGEMENT CENTER
7
VPN SERVICE MANAGER
2
PROVIDER NETWORK MANAGEMENT SYSTEM (P-NMS)
12
DATA COMMUNICATION NETWORK
PROVIDER NETWORK
DCN
CUSTOMER A USE IP-VPN MONITOR VIEW
IP-VPN SERVICE REQUEST
53
51
RAN
4
PE
52 (40)
MOBILE
8
CUSTOMER NETWORK MANAGEMENT CENTER
34
VPN SERVICE AGENT
3
13
CUSTOMER NETWORK MANAGEMENT SYSTEM (C-NMS)
DCN
CE
5
CUSTOMER NETWORK

FIG.26

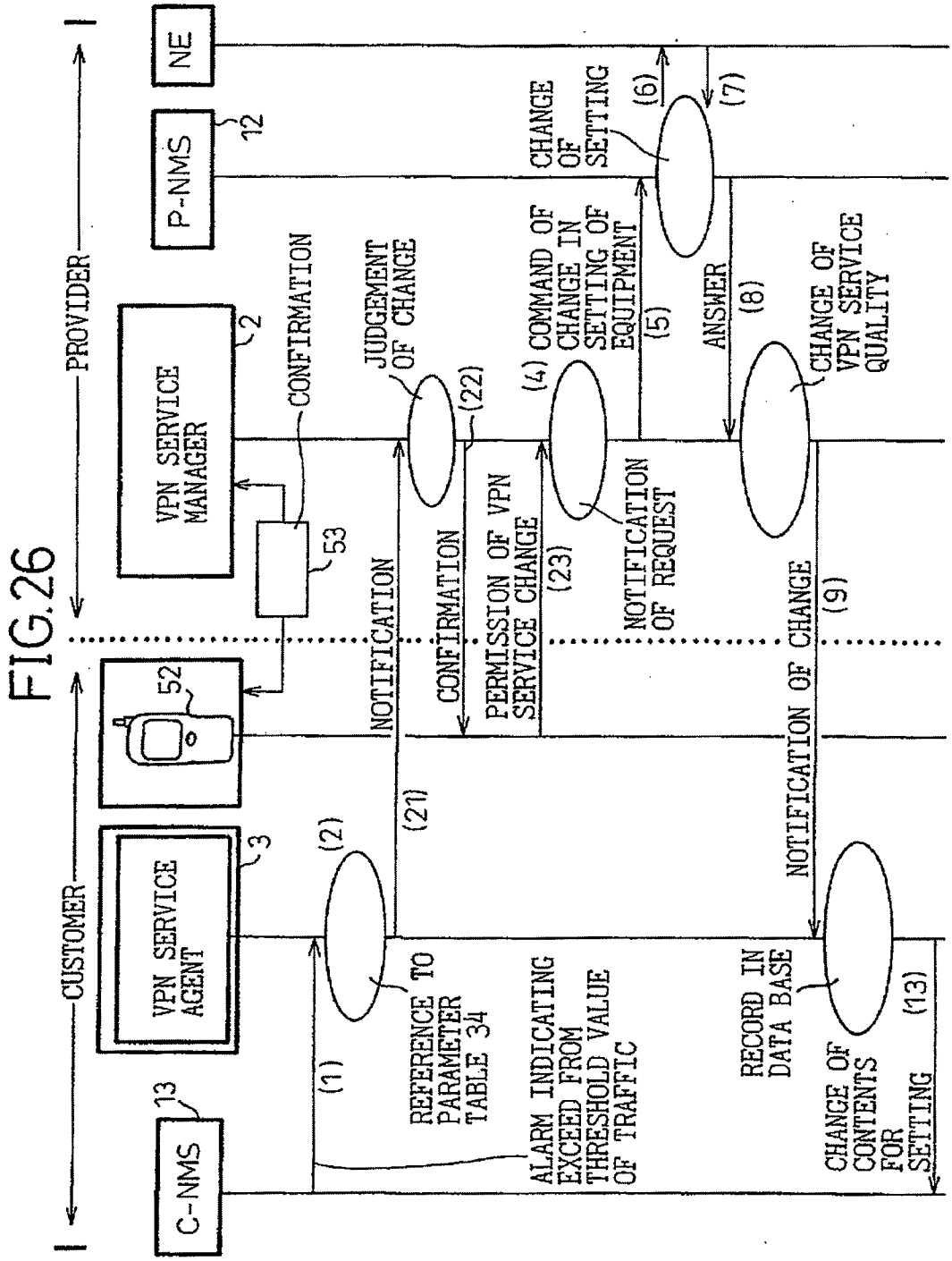

PROVIDER
CUSTOMER
NE
P-NMS
12
VPN SERVICE MANAGER
2
VPN SERVICE AGENT
3
C-NMS
13
52
53
CONFIRMATION
JUDGEMENT OF CHANGE
(22)
(4) COMMAND OF CHANGE IN SETTING OF EQUIPMENT
(5)
CHANGE OF SETTING
(6)
(7)
ANSWER
(8)
CHANGE OF VPN SERVICE QUALITY
NOTIFICATION
CONFIRMATION
PERMISSION OF VPN SERVICE CHANGE
(23)
NOTIFICATION OF REQUEST
NOTIFICATION OF CHANGE
(9)
(21)
(2)
(1)
REFERENCE TO PARAMETER TABLE 34
ALARM INDICATING EXCEED FROM THRESHOLD VALUE OF TRAFFIC
RECORD IN DATA BASE
CHANGE OF CONTENTS FOR SETTING
(13)

FIG.27

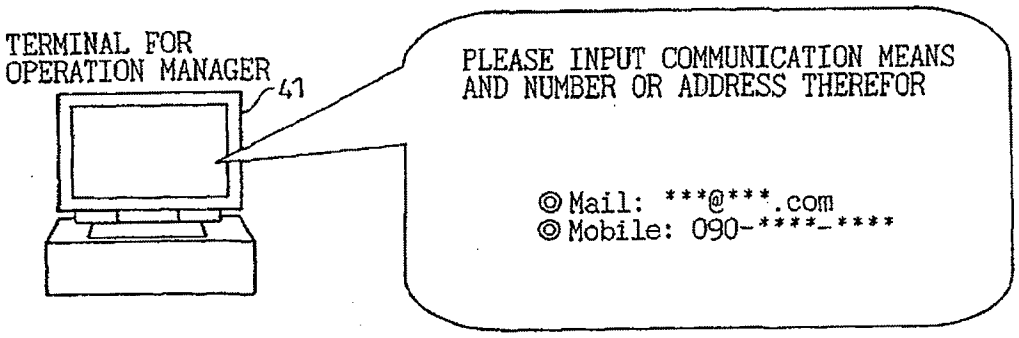

TERMINAL FOR
OPERATION MANAGER
41
PLEASE INPUT COMMUNICATION MEANS
AND NUMBER OR ADDRESS THEREFOR
◎Mail: ***@***.com
◎Mobile: 090-****-****

FIG.28

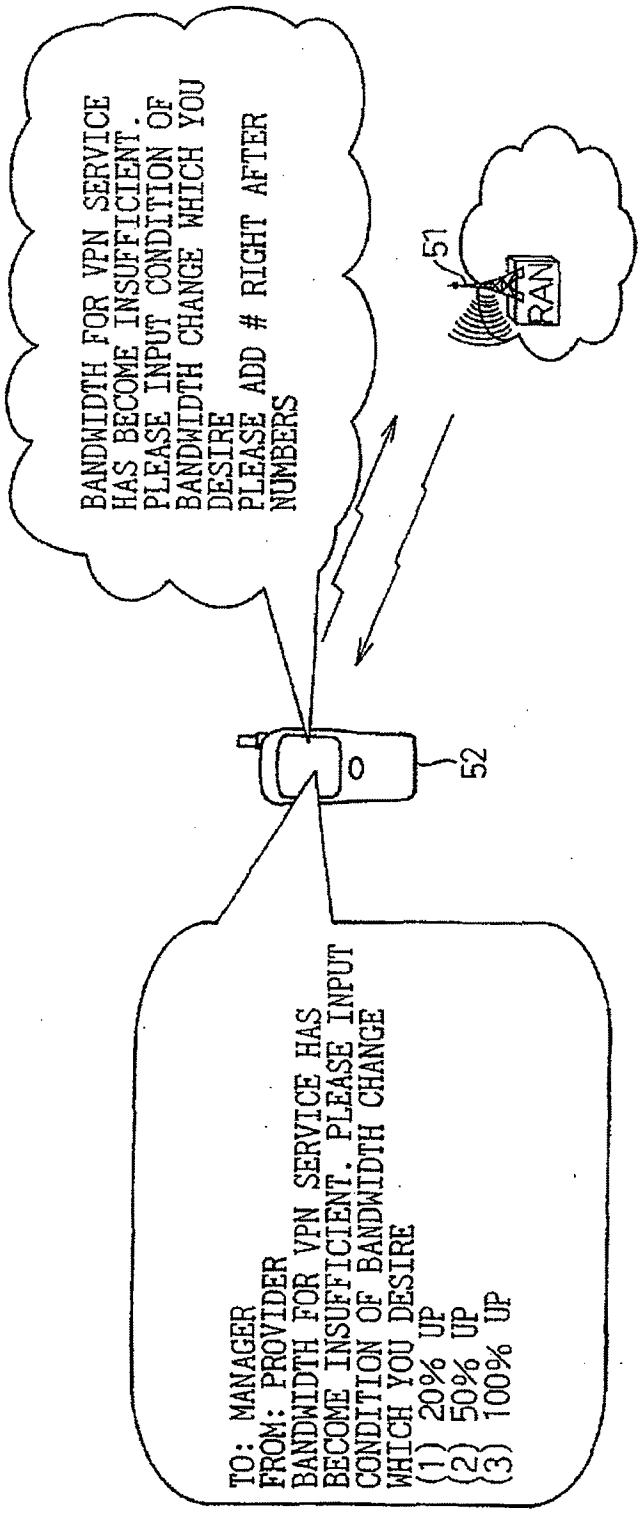

BANDWIDTH FOR VPN SERVICE HAS BECOME INSUFFICIENT. PLEASE INPUT CONDITION OF BANDWIDTH CHANGE WHICH YOU DESIRE
PLEASE ADD # RIGHT AFTER NUMBERS
51
RAN
52
TO: MANAGER
FROM: PROVIDER
BANDWIDTH FOR VPN SERVICE HAS BECOME INSUFFICIENT. PLEASE INPUT CONDITION OF BANDWIDTH CHANGE WHICH YOU DESIRE
(1) 20% UP
(2) 50% UP
(3) 100% UP

FIG.29

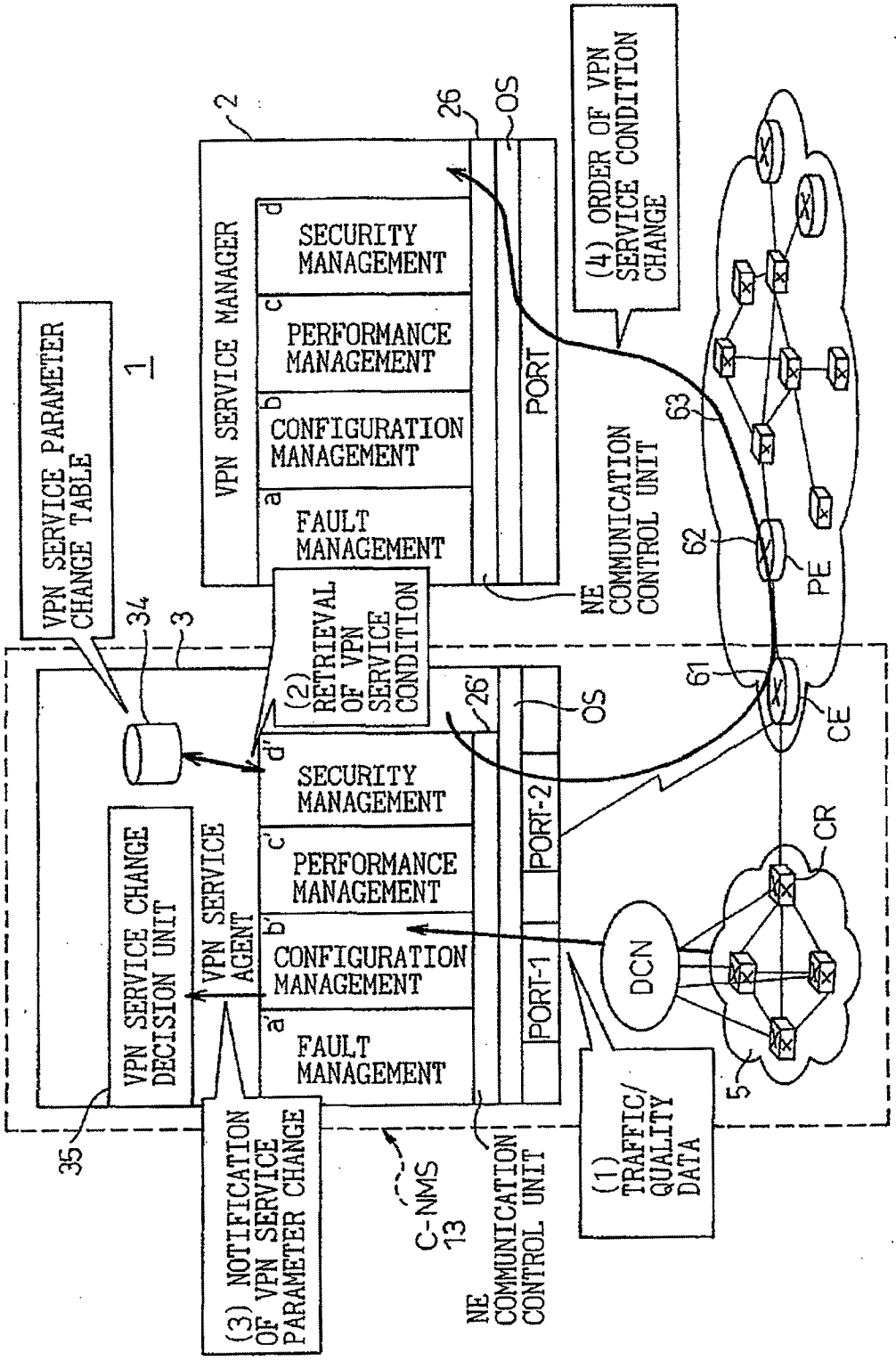

VPN SERVICE PARAMETER CHANGE TABLE
1
2
VPN SERVICE MANAGER
SECURITY MANAGEMENT
PERFORMANCE MANAGEMENT
CONFIGURATION MANAGEMENT
FAULT MANAGEMENT
26
OS
PORT
(4) ORDER OF VPN SERVICE CONDITION CHANGE
NE COMMUNICATION CONTROL UNIT
63
62
PE
61
CE
CR
5
34
3
(2) RETRIEVAL OF VPN SERVICE CONDITION
26'
OS
VPN SERVICE CHANGE DECISION UNIT
VPN SERVICE AGENT
SECURITY MANAGEMENT
PERFORMANCE MANAGEMENT
CONFIGURATION MANAGEMENT
FAULT MANAGEMENT
PORT-2
PORT-1
DCN
(1) TRAFFIC/ QUALITY DATA
35
(3) NOTIFICATION OF VPN SERVICE PARAMETER CHANGE
C-NMS 13
NE COMMUNICATION CONTROL UNIT

FIG.30

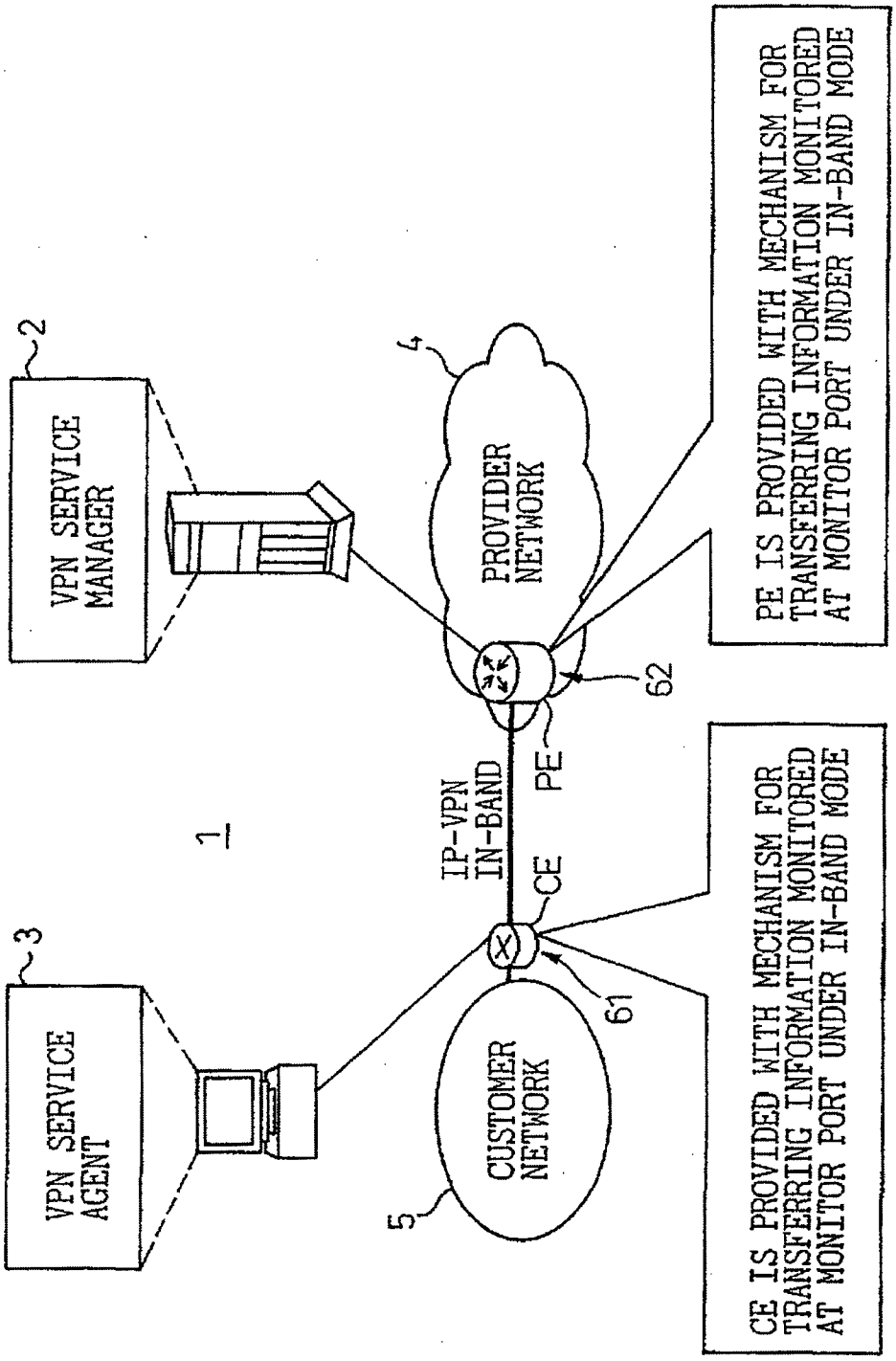

2
VPN SERVICE MANAGER
4
PROVIDER NETWORK
PE IS PROVIDED WITH MECHANISM FOR TRANSFERRING INFORMATION MONITORED AT MONITOR PORT UNDER IN-BAND MODE
62
PE
IP-VPN IN-BAND
CE
1
3
VPN SERVICE AGENT
CUSTOMER NETWORK
5
61
CE IS PROVIDED WITH MECHANISM FOR TRANSFERRING INFORMATION MONITORED AT MONITOR PORT UNDER IN-BAND MODE

FIG.31

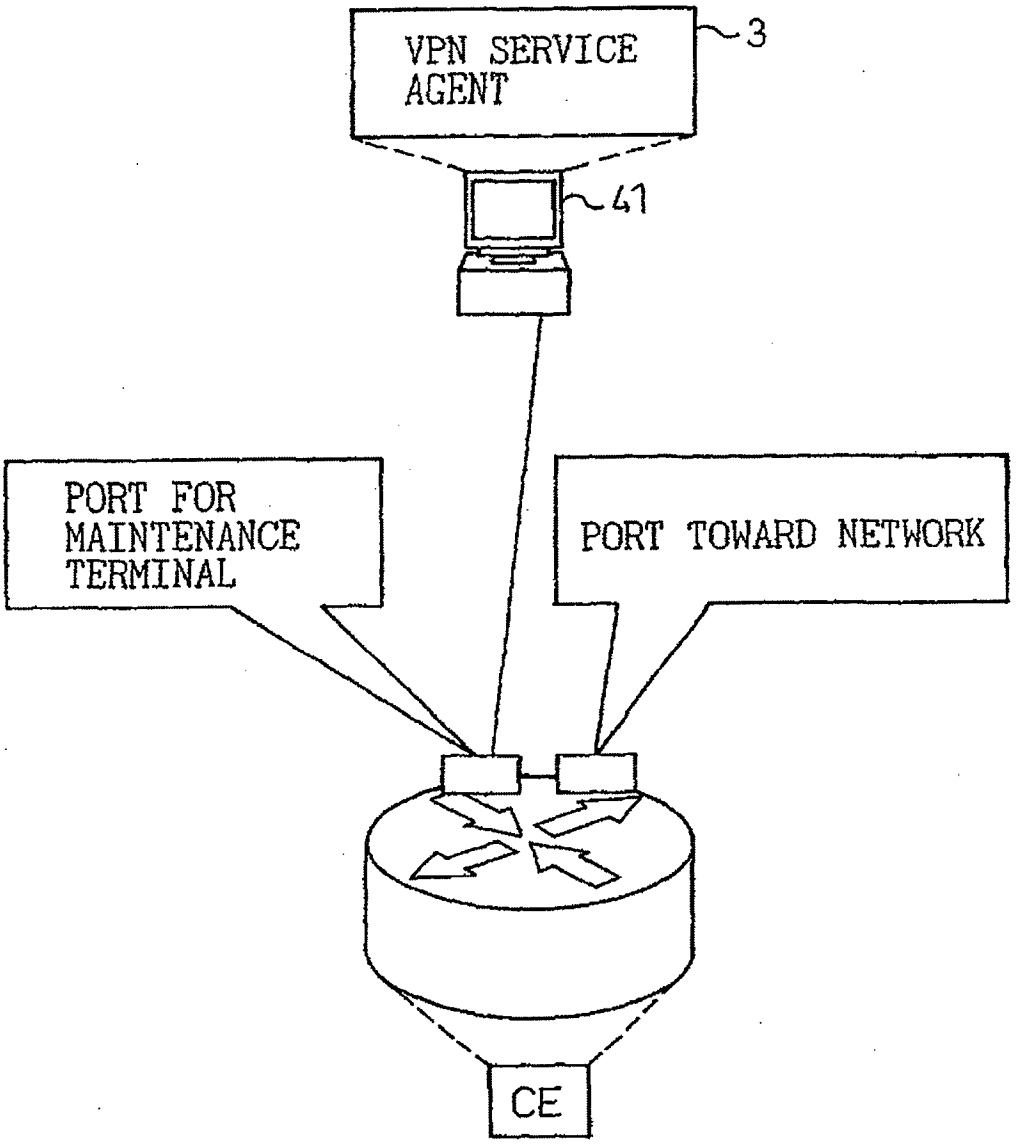

VPN SERVICE AGENT
3
41
PORT FOR MAINTENANCE TERMINAL
PORT TOWARD NETWORK
CE

FIG.32

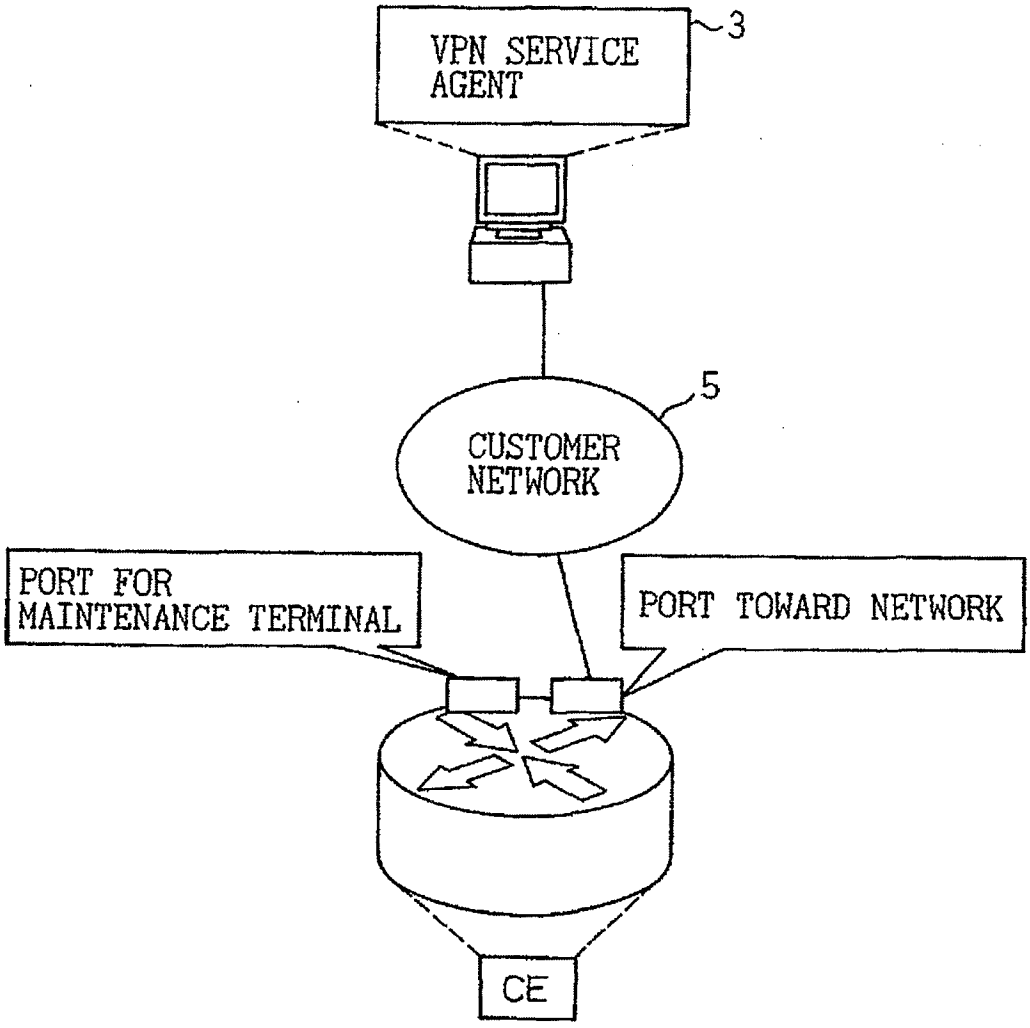
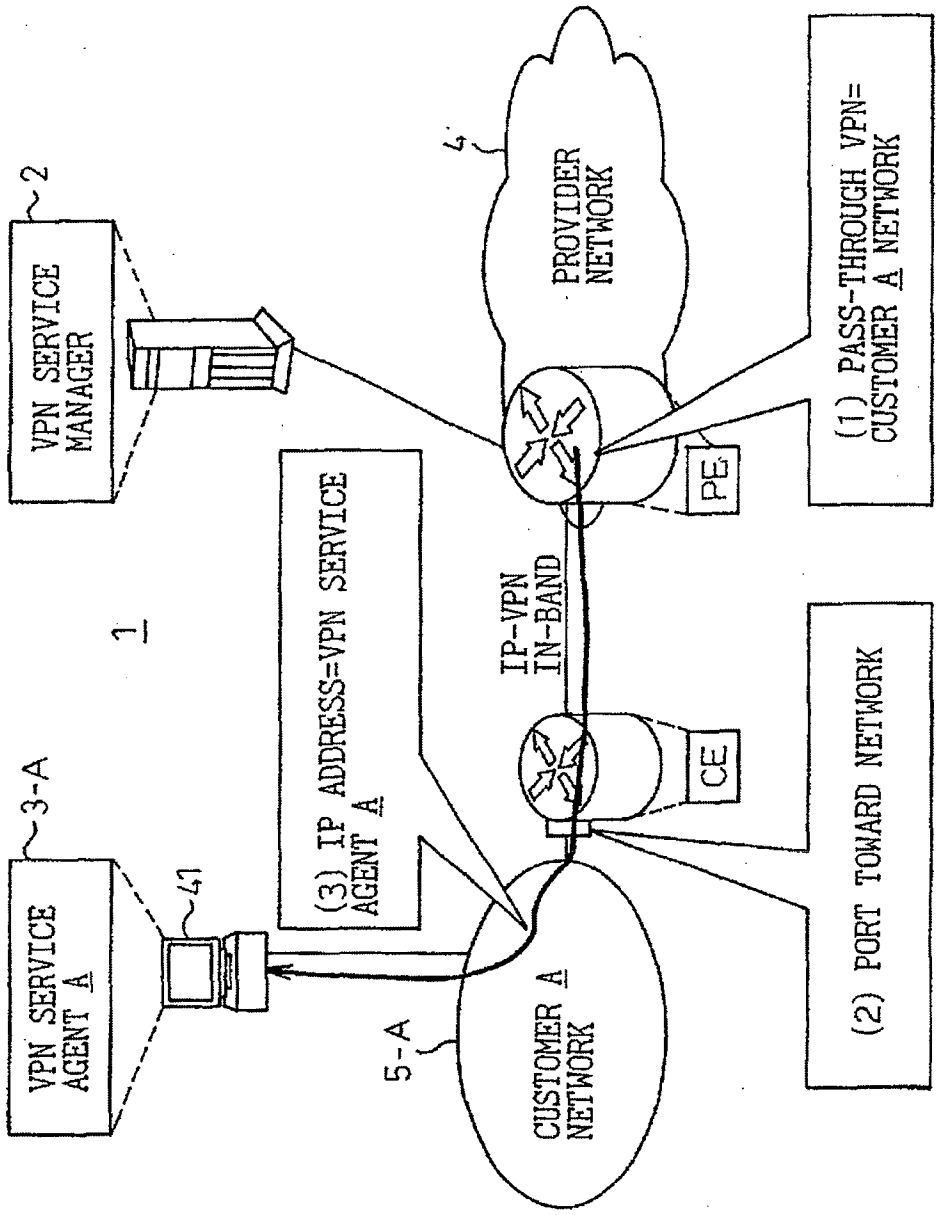

VPN SERVICE AGENT
3
CUSTOMER NETWORK
5
PORT FOR MAINTENANCE TERMINAL
PORT TOWARD NETWORK
CE

FIG.33


1
2
VPN SERVICE MANAGER
3-A
VPN SERVICE AGENT A
41
(3) IP ADDRESS=VPN SERVICE AGENT A
4
PROVIDER NETWORK
IP-VPN IN-BAND
PE
CE
(1) PASS-THROUGH VPN= CUSTOMER A NETWORK
(2) PORT TOWARD NETWORK
5-A
CUSTOMER A NETWORK

VPN SERVICE MANAGEMENT SYSTEM AND VPN SERVICE MANAGER AND VPN SERVICE AGENT COMPRISING SAME

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] The present invention relates to a virtual private network (VPN) service management system and to a VPN service manager and a VPN service agent comprising that system.

[0003] More particularly, the present invention relates to a mode of operation of a VPN service in a case where for example an Internet service provider (ISP), an application service provider (ASP), or a company having a plurality of places of business and operating an extra network among these places uses a VPN provided by a type 1 carrier so as to advance a widearea promotion of business. Note that, in the following explanation, a carrier providing a VPN service will be referred to as a "provider", and the ISP, ASP, company, etc. utilizing the VPN service will be referred to as "customers". Also, networks operated and managed by the provider and the customers will be referred to as a "provider network" and "customer networks", respectively.

[0004] 2. Description of the Related Art

[0005] Along with the various new services appearing one after another on the Internet, for example, on-line banking and Internet telephone, customers mainly utilizing the Internet in business have been increasingly calling for a higher speed and higher quality communications environment at low cost. In such a communications environment, it becomes indispensable to secure network security. Therefore, an IP-VPN capable of utilizing the Internet as a virtual dedicated line is now attracting attention. Providers have started to provide high quality communication services using such IP-VPN's according to their customer needs.

[0006] When a customer side uses this IP-VPN high quality communication service, it designates conditions regarding the desired-connecting nodes, guaranteed bandwidth, QoS, policy, data loss (packet loss), delay time, etc. at the time of contracting with the provider in advance and pays a fixed service usage fee in accordance with the contract conditions to the provider side in units of for example months. In this case, if desired, the customer side can change the contract conditions of the IP-VPN high quality communication service (hereinafter also simply referred to as a VPN service) from time to time usually with some charge.

[0007] Conventionally, when changing the contract conditions, (i) the customer or its agent applies for the change by means of for example the mail, facsimile, or telephone and makes arrangements for ordering the service from the provider, then (ii) an operator of the provider sets the VPN service conditions necessary for the change. By going through such a process, an environment capable of providing the intended service to a customer is prepared.

[0008] Summarizing the problem to be solved by the invention,-the procedure for changing the contract conditions between a customer and a provider conventionally took a predetermined period, for example, a few days to a few weeks, from application to when the changed service could be commenced. For this reason, there was the inconvenience that requests for changes of the VPN service usage conditions occurring sporadically or irregularly at the customer side such as in the following examples of use could not be dealt with timely:

[0009] 1) Example of use at a company: A president of a company wishes to circulate New Year's greetings or announce a rough medium term plan to all members of all places of business at one time via a company intranet.

[0010] 2) Example of use by ISP: The ISP wishes to double the bandwidths of its existing VPN's at one time for the start of the business of a new service.

[0011] 3) Example of use by ASP: The ASP wishes to prepare for a rush of applications when offering a Web ticket sale service, for example, only during a period of selling tickets for a popular group.

[0012] Also, the network management systems of a customer network and a provider network were configured completely independent from each other, so there was the problem in that the quality conditions or usage conditions of a VPN service could not be easily changed to deal with sudden changes of the VPN service conditions detected inside the customer network, for example, an increase of the traffic or amount of communication packets or a deterioration of an Internet access response performance.

[0013] Also, from the standpoint of the provider side, while facilities in the provider network for providing the VPN service can be investigated for the quality conditions, everything from the selection of models to management of the customer edge (CE) installed inside the customer network is entrusted to the customer side, so there was the problem in that it becomes difficult to fulfill a service level agreement (SLA) concluded at the time of contracting due to for example a later change of the model and specifications at the customer edge (CE) side.

SUMMARY OF THE INVENTION

[0014] An object of the present invention is to provide a VPN service management system for a IP-VPN service etc.

[0015] 1) capable of rapidly responding to a demand on the customer side to change the contract conditions between the customer and the provider,

[0016] 2) capable of easily changing the quality conditions or usage conditions of a IP-VPN service or other VPN service, and

[0017] 3) capable of always fulfiling a service level agreement concluded by a contract between the customer and the provider.

[0018] To attain the above object, the present invention provides a VPN service management system, for managing a VPN service for a communications network provided with a customer network (5) and a provider network (4), which has a VPN service manager (2) for managing the VPN service for the provider network (4) and a VPN service agent (3) for managing the VPN service for the customer network (5). This VPN service manager (2) changes the VPN service conditions in real time in accordance with an operation status of the customer network (5) in cooperation with the

VPN service agent (3). By this, a VPN service management system enabling a customer to rapidly and easily change the VPN service conditions is realized.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] The above object and features of the present invention will be more apparent from the following description of the preferred embodiments given with reference to the accompanying drawings, wherein:

[0020] **FIG. 1** is a view of the basic configuration of a VPN service management system according to the present invention;

[0021] **FIG. 2** is a view schematically showing a conventional typical VPN service network;

[0022] **FIG. 3** is a view schematically showing a VPN service network formed by the present invention;

[0023] **FIG. 4** is a view representing the entire VPN service management system according to the present invention;

[0024] **FIG. 5** is a view of the basic configuration of a VPN service management system 1 according to the present invention;

[0025] **FIG. 6** is a view of the configuration of **FIG. 5** using a concrete example;

[0026] **FIG. 7** is a view schematically representing a VPN service condition table;

[0027] **FIG. 8** is a view of the functions provided in a VPN service manager **2**;

[0028] **FIG. 9** is a view of the functions provided in a VPN service agent **3**;

[0029] **FIG. 10** is a first part of a flow chart for explaining a control sequence in **FIG. 6**;

[0030] **FIG. 11** is a second part of a flow chart for explaining the control sequence in **FIG. 6**;

[0031] **FIG. 12** is a view of an example of application of the present invention;

[0032] **FIG. 13** is a view of contents of a VPN service condition table **14** used in the example of application of **FIG. 12**;

[0033] **FIG. 14** is a first part of a view of a concrete image of the VPN service management system shown in FIG.

[0034] **FIG. 15** is a second part of a view of a concrete image of the VPN service management system shown in FIG.

[0035] **FIG. 16** is a view of the VPN service management system **1** for explaining a second embodiment (full automation) according to the present invention;

[0036] **FIG. 17** is a view of the concrete image of the VPN service management system **1** shown in **FIG. 16**;

[0037] **FIG. 18** is a view schematically showing a parameter table **34**;

[0038] **FIG. 19** is a view of a series of sequences under the second embodiment shown in **FIG. 16**;

[0039] **FIG. 20** is a view of the VPN service management system **1** for explaining a third embodiment (semi-automation) according to the present invention;

[0040] **FIG. 21** is a view of a series of sequences under the third embodiment shown in **FIG. 20**;

[0041] **FIG. 22** is a view of the VPN service management system **1** for explaining a fourth embodiment (server/client type) according to the present invention;

[0042] **FIG. 23** is a view of the concrete image of the VPN service management system **1** shown in **FIG. 22**;

[0043] **FIG. 24** is a view of a series of sequences under the fourth embodiment shown in **FIG. 22**;

[0044] **FIG. 25** is a view of the VPN service management system **1** for explaining a fifth embodiment (remote permission response type) according to the present invention;

[0045] **FIG. 26** is a view of a series of sequences under the fifth embodiment shown in **FIG. 25**;

[0046] **FIG. 27** is a view schematically representing a connection method to an operation manager;

[0047] **FIG. 28** is a view schematically representing advance preparations with the operation manager;

[0048] **FIG. 29** is a view of the configuration of **FIG. 17** with the sixth embodiment applied thereto;

[0049] **FIG. 30** is a view explaining an in-band means according to the present invention;

[0050] **FIG. 31** is a view of a first connection method between a customer edge and an agent **3**;

[0051] **FIG. 32** is a view of a second connection method between the customer edge and the agent **3**; and

[0052] **FIG. 33** is a view of an example of the connection by the in-band between the manager **2** and the agent **3**.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0053] Preferred embodiments of the present invention will be described in detail below while referring to the attached drawings.

[0054] **FIG. 1** is a view of the basic configuration of the VPN service management system according to the present invention.

[0055] In the figure, reference numeral **1** indicates the VPN service management system. This is a VPN service management system for managing a VPN service for a communication network provided with a customer network **5** for servicing customers and a provider network **4** constructed by the provider for providing the VPN service to the customers and connected to the customer network **5**. The system **1** has at least a VPN service manager **2** for managing the VPN service for the provider network **4** and a VPN service agent **3** for managing the VPN service for the customer network **5**.

[0056] Here, the VPN service manager **2** is configured so as to change the VPN service conditions of the VPN service to be provided by the system **1** in real time in accordance with the operation status of the customer network **5** under

the management of the VPN service agent 3 in cooperation with the VPN service agent 3.

[0057] Due to the above configuration, the above-mentioned first problem of the related art that a contract of a VPN service cannot be rapidly changed, the second problem that the quality conditions or usage conditions of the VPN service (VPN service condition) cannot be easily changed, and the third problem such that it is difficult to always fulfill the service level agreement can be solved. This will be explained in detail below.

[0058] In order to facilitate understanding of the present invention, the intention of the present invention will be clarified first by explaining the present invention as a whole, then components of the present invention will be individually explained.

[0059] **FIG. 2** is a view schematically showing a conventional typical VPN service network.

[0060] In the figure, reference numeral **6** is a carrier network and represents a scope of management of the carrier in a general leased line service.

[0061] This carrier network **6** has a plurality of customer networks **5** arranged under it. In the example of the figure, customer A networks **1**, **2**, **3**, and **4** in each of which the customer A has four nodes are shown.

[0062] In order to construct the VPN service network among these customer networks **5** centered about the carrier network **6**, an illustrated customer A leased line network is formed. This customer A leased line network is formed between customers via provider edges (PE's) and provider core routers (PCR's) in the carrier network **6** and the customer edges (CE's) and the customer routers (CR's) in the customer networks **5**. Contrary to this, the VPN service network of the present invention is constructed as follows.

[0063] **FIG. 3** is a view schematically showing a VPN service network formed by the present invention. It shows this based on the configuration of **FIG. 2**. Note that similar components are indicated by the same reference numerals or symbols throughout all of the figures.

[0064] When comparing **FIG. 2** and **FIG. 3**, there is a difference between the two in the point that the customer edge (CE) under the management of each customer network **5** in **FIG. 2** is also placed under the management of the carrier network side in **FIG. 3**. Namely, in the provider network **4** of the present invention, the original scope of management of the carrier network is extended up to the customer side. By this, it becomes possible to control the VPN service conditions through the customer edges. On the other hand, for this, on the provider side, an illustrated provider network management system (P-NMS) **12** becomes a useful managing means, while on the customer side, an illustrated customer network management system (C-NMS) **13** becomes a useful managing means. Note that, as little as one C-NMS is sufficient for the customer A networks **1**, **2**, **3**, and **4**.

[0065] According to the VPN service network shown in **FIG. 3**, the business merits shown in following [1] to [3] can be expected.

[0066] First, from the viewpoint of the provider side,

[0067] [1] A 24-hour monitoring service (outsourcing) of the customer VPN network including the customer edges (CE's) can be realized;

[0068] [2] Greater uniformity of the VPN service and the VPN service conditions thereof can be achieved and, as a result, it becomes unnecessary to deal with specifications differing for every vender model in the customer edges (CE's).

[0069] Also, from the viewpoint of the vender side, in addition to above [1] and [2],

[0070] [3] one vender can continuously supply customer edges (CE's), provider management system (P-NMS) and customer management system (C-NMS), unique to the vender, for one provider under contract with this provider.

[0071] A VPN service management system offering the business merits shown in the above [1], [2], and [3] will be explained next.

[0072] **FIG. 4** is a view of the overall VPN service management system according to the present invention. The figure shows the system configuration of **FIG. 1** mentioned above as a reality-based concrete example.

[0073] In **FIG. 4**, the VPN service manager **2** shown in **FIG. 1** is housed in a provider network management center **7**. Also, the center **7** houses the provider network management system (P-NMS) **12** mentioned above. Note that, in the figure, as an example, two systems P-NMS1 and P-NMS2 are shown. This is for considering various business applications.

[0074] On the other hand, in **FIG. 4**, the VPN service agent **3** shown in **FIG. 1** is housed in the customer network management center **8**. Also, the center **8** houses the above mentioned customer network management system (C-NMS) **13**.

[0075] The VPN service management system **1** according to the present invention is constructed by the above components, the provider network **4**, and the customer network **5** working together.

[0076] The point which must be particularly noted in this VPN service management system **1** is that the following three requirements <1>, <2> and <3> can be satisfied. These three requirements could not be satisfied with the conventional VPN service.

[0077] Namely, according to the VPN service management system **1** of the present invention, the following requirements are satisfied:

[0078] <1> That the VPN service conditions (quality conditions or usage conditions of the VPN service) provided from the provider side can be instantly changed by the customer side (for example, corporate user side),

[0079] <2> That the VPN service conditions can be easily changed in accordance with the traffic characteristics and the usage mode of the VPN in a customer network **5** automatically or by designating a time, and

[0080] <3> That the settings of the VPN service conditions can be controlled by the customer (for example corporate user) by using the VPN contracted with the provider by the customer (by using for example an in-band communication mode).

[0081] Also, by satisfaction of the above three requirements <1 >, <2> and <3>, it becomes possible to meet the three customer (for example, corporate user) side demands 1), 2), and 3) mentioned above. Namely,

[0082] 1) Example of use at a company: A president of a company wishes to circulate New Year's greetings or announce a rough medium term plan to all members of all places of business at one time via a company intranet,

[0083] 2) Example of use by ISP: The ISP wishes to double the bandwidths of its existing VPN's at one time for the start of the business of a new service, and

[0084] 3) Example of use by ASP: The ASP wishes to prepare for a rush of applications when offering a Web ticket sale service, for example, only during a period of selling tickets for a popular group.

[0085] Referring to **FIG. 4** again here, the flows of processing corresponding to the above requirements <1>, <2>, and <3> are shown as routes R<1>, R<2>, and R<3> in the figure.

[0086] In the route R<1>, the VPN service manager 2 provides a VPN service menu to the VPN service agent 3. This menu displays the various types of the VPN service which can be provided to the customers.

[0087] Also, in the route R<1>, the VPN service agent 3 considers the state of use of the VPN's of the customer networks 5 under it and refers to the menu to request the desired VPN service to the VPN service manager 2.

[0088] In the route R<2>, the VPN service agent 3 collects information concerning the traffic characteristics and the usage mode of the VPN's in the subordinate customer networks 5 via the C-NMS 13 and generates an illustrated VPN service demand in the route R<1>.

[0089] In the route R<3>, the collected information concerning the traffic characteristics and usage mode of the VPN's is actually reflected at the provider side. Namely, the information is transmitted to the provider side. This transmission is achieved from the C-NMS 13 through the customer edges (CE) by using VPN's in contract under the in-band mode.

[0090] First Embodiment

[0091] Details of the VPN service management system 1 satisfying the above requirements <1>, <2>, and <3> will be concretely explained next.

[0092] **FIG. 5** is a view of the fundamental configuration of the VPN service management system 1 according to the present invention. Accordingly, most of the configuration of the figure is included in the configuration of **FIG. 4**.

[0093] The parts of the configuration which should be noted in the figure are as follows.

[0094] The system 1 further has a provider network management system (P-NMS) 12 cooperating with the VPN service manager 2 on the provider side. This provider network management system 12 manages the provider network 4 including also the customer edges (CE's) arranged in the customer networks 5 for connection with the provider network 4.

[0095] The system 1 may be provided with, at least, the provider network management system (P-NMS) 12 in addition to the VPN service manager 2 and the VPN service agent 3. In order to further impart various functions, however, preferably the above mentioned customer network management system (C-NMS) 13 is disposed, although it is not shown in **FIG. 5**. Namely, the system 1 further has a customer network management system (C-NMS) 13 cooperating with the VPN service agent 3 and managing the customer network 5 on the customer side. This customer network management system 13 monitors the customer edges (CE's) and communicates with the provider network 4 side.

[0096] According to the example of **FIG. 5**, the VPN service manager 2 provides the customer A with an IP-VPN monitor view for the customer A network as the above mentioned VPN service menu. The customer A makes a request for the desired IP-VPN service via the VPN service agent 3 to the provider side according to this IP-VPN monitor view. Note that, in the figure, illustration of other customer A networks (refer to **FIG. 3**) linked with this customer A network is omitted. A network configuration wherein, if for example the illustrated customer A network is located in Tokyo, the other customer A networks are located in Hokkaido, Nagoya, Osaka, Kyushu, etc. is considered. The configuration of **FIG. 5** will be further concretely explained next.

[0097] **FIG. 6** is a view of a concrete example of the configuration of **FIG. 5**.

[0098] The schematic configuration of the figure will be explained next. Note that, in the figure, E1, E2, E3, . . . represent various types of events. These events will be explained in detail by referring to **FIG. 10** and **FIG. 11** mentioned later.

[0099] In **FIG. 6**, P-ip is the provider side IP network of the VPN service. C-ip1 and C-ip2 are IP networks of the customer side of the VPN service and are connected to P-ip. This P-ip has connected to a plurality of customer side IP networks of the VPN service. Here, a "VPN service" means a service based on existing technology wherein a provider side IP network relays information among a plurality of partial customer IP networks without processing so as to realize a single virtual customer IP network overall comprised of the customer IP networks.

[0100] The customer edges (CE's) are the customer side IP apparatuses of the VPN service for connecting the customer IP networks of the VPN service and the provider IP network of the VPN service. Also, "PE" shows a provider side IP apparatus of the VPN service connected to a customer edge (CE).

[0101] The provider network management system P-NMS12 is a provider side IP apparatus which monitors and controls the IP network. This P-NMS12 monitors and controls the operation status of the provider IP apparatus and the IP network.

[0102] The customer network management system C-NMS12 is a customer side IP apparatus which monitors and controls the IP network. This C-NMS12 monitors and controls the operation status of that customer IP network.

[0103] Any numbers of these P-NMS12 and C-NMS12 may be disposed according to the scale of the IP apparatuses and IP networks to be managed, the geographic conditions, operation conditions, etc.. Here, each C-NMS12 can monitor and control a customer edge (CE), while the P-NMS12 can monitor and control customer edges (CE) through the C-NMS12's or through the provider side IP apparatuses (PE).

[0104] In the present invention, a VPN service manager 2 able to control the VPN service for the customer edges (CE) disposed on the C-ip network is provided in the P-NMS12.

[0105] Also, a VPN service agent 3 for enabling a customer side VPN service operator to remotely control the VPN service manager 2 is provided in each C-NMS12.

[0106] The VPN service manager 2 and each VPN service agent 3 cooperate by the interposition of a VPN service condition table between them. This table will be explained below.

[0107] **FIG. 7** is a view schematically showing the VPN service condition table.

[0108] The VPN service manager 2 provides a service menu concerning the VPN service as the VPN service condition table 14 in the figure to the VPN service agent 3. When there is a request for change of the VPN service conditions on the customer side, the VPN service agent 3 transmits the request for change to the VPN service manager 2 via that service menu. The VPN service manager 2 then reflects the request for change in the provider network 4 via the provider network management system 12.

[0109] For example, this VPN service condition table 14 is arranged in the P-ip network or the P-NMS12 of **FIG. 6**. This VPN service condition table 14 holds identifiers of the VPN service customers and VPN identifiers allocated to the concerned customers, CE identifiers for identifying the customer edges CE of the two end points (end point A to end point Z) of the VPN and arranged at the target customers, a list of VPN service condition items which can be changed by the VPN service customers, current values set, at present, in correspondence with the items of the VPN service conditions, and allowable maximum/minimum values allowed as the VPN service condition values and setpoint bandwidths (bandwidths to be used) thereof. Sometimes items of the VPN service conditions and the range of allowable values are stipulated in the VPN service contract between the customer and the provider, while other times items of the VPN service conditions are added or deleted in accordance with the situation of the VPN service or the state of the IP network. Note that these VPN service condition items sometimes differ for different technical specifications for realizing the VPN service. Explaining this further, at times of a major disaster, it becomes impossible to stipulate a guaranteed band. The VPN service condition stipulating the bandwidth may be deleted or, conversely, a VPN service condition that a leased line such as a wireless or satellite channel be used to enable bandwidth to be secured with priority, that is, routing through a leased line, can be added.

[0110] By interposing the VPN service condition table 14 as described above, the VPN service manager 2 and the VPN service agents 3 can cooperate with each other. The means (functions) which must be provided in the VPN service manager 2 and VPN service agents 3 for this cooperation will be explained next.

[0111] **FIG. 8** is a view of the functions provided in the VPN service manager 2, while **FIG. 9** is a view of the function provided in the VPN service agents 3.

[0112] Referring to **FIG. 8**, the VPN service manager 2 is provided with

[0113] a VPN service order control means 21 for receiving an order when an order for changing the VPN service conditions (**FIG. 7**) is generated from a VPN service agent 3 and outputting the changed VPN service conditions concerned in that order,

[0114] a VPN service condition retrieval means 22 for retrieving the present VPN service conditions given to the concerned customer network 5 from the VPN service condition table (**FIG. 7**) when that order is generated,

[0115] a VPN service condition decision means 23 for deciding whether or not the range by which the changed VPN service conditions exceed the present VPN service conditions is within an allowable range,

[0116] a VPN service condition setting means 24 for resetting the present VPN service conditions to the changed VPN service conditions when the result of said decision is "POSSIBLE", and

[0117] a customer edge control means 25 for controlling the customer edge (CE) based on the reset VPN service conditions.

[0118] By this means 25, the provider side VPN service operator becomes able to control the VPN service at the customer edge (CE).

[0119] Further supplementing the explanation, the VPN service order control means 21 receives an order for changing the VPN service conditions (VPN service order) from a VPN service agent 3. Based on the customer identifier and the VPN identifier contained in the concerned order, individual VPN service conditions and values similarly contained in the concerned order are transferred to the VPN service condition decision means 23.

[0120] When the result of decision by the service condition decision means 23 is "POSSIBLE", the VPN service condition setting means 24 is used to change the present values of the VPN service condition table 14.

[0121] Thereafter, the VPN service conditions and values are converted to control information corresponding to the customer edge (CE), then the control information is transmitted to the CE control means 25. Further, based on the result of decision by the VPN service condition decision means 23 and the result of the control by the CE control means 25, the result is sent back to the VPN service agent 3.

[0122] The VPN service condition retrieval means 22 extracts the contents of the VPN service condition table 14 for the customer identifier and the VPN identifier.

[0123] The VPN service condition decision means **23** confirms for each of the individual VPN service conditions and values thereof contained in the VPN service condition change order whether or not the VPN service condition table **14** has the corresponding VPN service condition and whether or not the corresponding value is within the allowable values based on the customer *identifier* and VPN identifier.

[0124] The VPN service condition setting means **24** sets the values contained in the VPN service order as the present values for the individual VPN service condition items based on the customer identifier and the VPN identifier.

[0125] Referring to **FIG. 9** next, each VPN service agent **3** is provided with

[0126] a VPN service condition retrieval means **31** for retrieving the current VPN service conditions given to a concerned customer network **5** from the VPN service condition table **(FIG. 7)** when an order for changing the VPN service conditions is generated from a customer and

[0127] a VPN service order issuing means **32** for issuing the order to the VPN service manager **2** based on the retrieved VPN service conditions.

[0128] Also, the VPN service agent **3** is provided with a customer edge control means **33** for controlling the customer edge (CE) based on the VPN service conditions reset by the VPN service manager **2** upon receipt of the order when the VPN service manager **2** controls the customer edge (CE) through the VPN service agent **3**.

[0129] Note that a group of functions for collecting IP network information for issuing a change of VPN service conditions (VPN service order) such as monitoring for faults and monitoring traffic of the C-ip network **(FIG. 6)** is arranged in the C-NMS12.

[0130] Further supplementing the explanation, the VPN service order issuing means **32** issues an order for changing the values of the individual VPN service conditions to the VPN service manager **3** based on the IP network information obtained from the C-NMS12.

[0131] The customer edge control means **33** controls the functions relating to the VPN service provided in the customer edge (CE).

[0132] Returning to **FIG. 6** again, the above mentioned events E1, E2, E 3, . . . will be explained in the form of a control sequence based on the explanation given with reference to **FIG. 7**, **FIG. 8**, and **FIG. 9**.

[0133] **FIG. 10** and **FIG. 11** are parts of a flow chart for explaining the control sequence in **FIG. 6**.

[0134] First, the correspondence between the steps (S11 to S19) of **FIG. 10** and **FIG. 11** and the events (E1 to E5) of **FIG. 6** becomes as follows:

[0135] E1: S11, S12, and S13

[0136] E2: S14

[0137] E3: S15, S16, and S17

[0138] E4: S18

[0139] E5: S19

[0140] Steps S11 to S19 are as follows.

[0141] Step S11: The VPN service manager of the C-ip network judges the change of the VPN service conditions from the C-ip network information of the C-NMS12 and the predetermined network operation schedule.

[0142] Step S12: The VPN service condition retrieval means **31** of the VPN service agent **3** acquires the VPN service conditions of the concerned customer.

[0143] Step S13: The VPN service manager of the C-ip network issues a VPN service order to the VPN service agent **3**.

[0144] Step S14: The VPN service order issuing means **32** of the VPN service agent **3** transmits the VPN service order to the VPN service manager **2**.

[0145] Step S15: The VPN service order control means **21** of the VPN service manager **2** issues the VPN service order to the VPN service condition decision means **23**.

[0146] Step S16: It is decided whether the result of the decision is "POSSIBLE" (OK) or "IMPOSSIBLE" (NG).

[0147] Step S17: The CE control means **25** of the VPN service manager **2** controls the customer edge (CE) based on the VPN service order.

[0148] Step S18: The VPN service manager **2** sends back the result of the VPN service order to the VPN service agent **3**.

[0149] Step S19: The VPN service manager **2** notifies the result of the VPN service order to the adjoining VPN service agent **3**.

[0150] By the above configurations **(FIG. 7, FIG. 8,** and **FIG. 9)** and the control sequences **(FIG. 10** and **FIG. 11),** the VPN service operator of the customer side IP network becomes able to change the VPN service conditions freely and dynamically without going through the VPN service operator of the provider side IP network. This means that the VPN service operator of the VPN service customer side can efficiently operate the customer IP network on a timely basis based on the usage situation and predictions of the virtual customer IP network as a whole.

[0151] **FIG. 12** is a view of an example of application of the present invention, while **FIG. 13** is a view of the contents of the VPN service condition table **14** used in the example of application of **FIG. 12**.

[0152] Note that **FIG. 12** should be viewed in substantially the same way as **FIG. 6**, and **FIG. 13** is a detailed example of the VPN service condition table **14** shown in **FIG. 7**. The table **14** is formed in the database (DB) **15** of **FIG. 12**.

[0153] An example of application of the present invention will be explained by referring to **FIG. 12** and **FIG. 13**.

[0154] A certain customer, that is, a company ci offering a Web ticket sale service, has two customer IP networks cip1 and cip2 monitored and controlled by a single customer network management system C-NMS12. A VPN service is provided between the cip1 and cip2 by the provider IP network P-ip.

[0155] At this time, the customer edges are CE1 and CE2, the provider edges are PE1 and PE2, and the provided VPN

is a VPNci reaching CE2 from CE1 via PE1 and PE2. Also, an example is shown wherein the database (DB) **15** for storing the VPN service condition table **14** is disposed in the P-NMS12.

[0156] As the VPN service condition with respect to this VPNci provided to the company ci, the bandwidth of the VPN service can be freely changed. The current value of that bandwidth, maximum value, minimum value, and the set-point bandwidth are bw-i, bw-max, bw-min, and bwA (bw: bandwidth) as shown in **FIG. 13**. The customer identifier and VPN identifier of the company ci in this case are ci-id and VPNci-id, while the CE identifiers of the two end points (A, Z) of the VPNci, that is, CE1 and CE2, are CE1-id and CE2-id.

[0157] Note that, in order to realize the VPN service, other than what is described above, there is a lower rank network technology for realizing VPN links between CE1 and PE1, between PE1 and PE2, and between PE2 and CE2 and VPN.

[0158] Here, during the ticket sale period, orders from persons who desire to purchase tickets rush in. Therefore, the amount of accesses to the VPNci (that is, between cip1 and cip2) suddenly increases. For this reason, the VPN service conditions will be rapidly changed. The control in this case becomes as follows.

[0159] 1. The VPN service manager of the VPNci decides that a change of the VPN service bandwidth is necessary at the start of the ticket sales.

[0160] 2. The VPN service manager acquires the VPN service conditions (VPN service bandwidth) of the VPNci from the database (DB) **15** by the VPN service condition retrieval means **31** of the VPN service agent (VPNa) **3** and determines that the bandwidth bw should be increased by exactly bw'.

[0161] 3. The VPN service manager issues an order for changing the VPN service bandwidth corresponding to the customer identifier ci and the VPN identifier VPNci-id from bw to bw' to the service agent (VPNa) **3**.

[0162] 4. The VPN service order issuing means **32** of that service agent VPNa transmits that order to the VPN service manager (VPNm) **2**.

[0163] 5. The VPN service order control means **21** of this service manager VPNm issues the concerned order to the VPN service condition decision means **23**.

[0164] 6. This VPN service condition decision means **23** evaluates whether or not the changed bandwidth bw' contained in that order satisfies the following conditions with respect to bw-max and bw-min in the database **15**.

$$bw\text{-}min < bw' < bw\text{-}max$$

[0165] The VPN service condition decision means **23** returns the result of the decision "OK" for that order if the above conditions are satisfied, but will return the result of the decision "NG" if the above conditions are not satisfied (step S16 of **FIG. 7**).

[0166] 7. When the result of the decision received from the VPN service condition decision means **23** is "OK", the VPN service order control means **21** issues the concerned order to the VPN service condition setting means **24**, but when the result of the decision received from the VPN service condition decision means **23** is "NG", it responds that the order has failed to the agent VPNa and the present control is terminated.

[0167] 8. The VPN service condition setting means **24** changes the present value of the VPN service bandwidth as the service condition imparted to VPNci from bw to bw'.

[0168] 9. Further, the VPN service order control means **21** controls CE1 and CE2 to change bw to bw' by using the CE control means **25** when the result of the decision at the above 7. is "OK".

[0169] 10. The VPN service order control means **21** returns the result of control of the CE1 and CE2 at the above 9. as a response to the agent VPNa.

[0170] 11. At the end of the ticket sale, control is performed so that the order becomes bw at the above 2. to 10. to change the VPN service bandwidth from bw' to the original bw again.

[0171] Due to the above, during the ticket sale period by the company ci, it is possible to increase the VPN service bandwidth of the VPNci so as to deal with the rush in access by persons who desire to purchase tickets.

[0172] A concrete image of the system shown in **FIG. 1** will be shown next supplementarily by using the figures. **FIG. 14** and **FIG. 15** are parts of a view of a concrete image of the VPN service management system shown in **FIG. 1**.

[0173] In **FIG. 14**, the right side (provider side) and left side (customer side) show the VPN service manager **2** and a VPN service agent **3** of the VPN service management system **1**.

[0174] As the main function of the VPN service manager **2**, the VPN service order control function (refer to means **21** of **FIG. 8**) is shown. As the original operation for achieving this function, the VPN service manager **2** performs the illustrated policy control, QoS (Quality of Service) management, stock management, etc. "Stock management" means so-called "resource management" for deciding whether or not a demand for increase can be accepted when receiving a demand to suddenly increase the bandwidth, for example, to 100 Mbps from a customer operating with a bandwidth of 10 Mbps at present.

[0175] Also, the provider network management system (P-NMS) 12cooperating with that VPN service manager **2** has at least the illustrated units for management of faults (a), configuration (b), performance (c), and security (d). The VPN service manager **2** controls network elements (NE) such as the PE's, CE's, and PCR's in the subordinate provider network **4** via the NE communication control unit **26** and corresponding ports under the operating system (OS) in the system (P-NMS) 12 based on the management data by these management units a to d.

[0176] The fault management unit a watches constantly faults occurring in the provider network **4**.

[0177] The configuration management unit b watches constantly what kind of network elements (NE) the provider network **4** is configured by.

[0178] The performance management unit c constantly monitors the traffic information and amount of generation of packet loss in the network elements.

[0179] Also, the security management unit d makes security checks by passwords and authentication.

[0180] On the other hand, the main functions of the VPN service agent 3 provided at the left side (customer side) of **FIG. 14** are shown as a function of monitoring the traffic of the customer edge (CE), a function of controlling requests for quality of VPN service, and a function of monitoring faults at the customer VPN. The customer edge CE is monitored via the corresponding port under the operating system (OS).

[0181] The processing in the VPN service management system 1 shown in **FIG. 14** may be roughly classified to following processing (1), (2), and (3). Note that, (1), (2), and (3) are shown also in **FIG. 14**.

[0182] (1) For example, when the president of a company, that is, the customer A, wishes to broadcast a management plan to all employees at all places of business of the company all together through the customer A networks 1, 2, 3, and 4 of **FIG. 3**, the concerned VPN service agent 3 requests a change of the customer VPN service conditions at the VPN service manager 2. That is, it requests a temporary increase of the bandwidth (bw).

[0183] (2) The VPN service manager 2 receiving that request requests a change of the VPN service conditions at the subordinate provider network management system (P-NMS) 12.

[0184] (3) The provider network management system 12 receiving that request sends a command indicating that "the VPN service conditions be changed" to the network elements (NE) in the subordinate provider network 4.

[0185] Next, refer to **FIG. 15**. The figure shows a more realistic image of the configuration of **FIG. 14**.

[0186] In **FIG. 15**, the VPN service agent 3 is shown as having the function of issuing a VPN service order (refer to the means 32 of **FIG. 9**) and a function of retrieving the VPN service conditions (refer to the means 31 of **FIG. 9**).

[0187] e shown at the top left of the figure is the VPN service quality demand menu. This menu e is the menu for specifying the service for which provision is sought from the customer side from the list of services which can be provided by the manager 2 presented from the VPN service manager 2 and returning it to the manager 2.

[0188] Further, g is the CE traffic view for checking the change in traffic over time at the customer edge (CE) on the customer side. By referring to this traffic view g, the operation manager of the customer side can determine the present situation of the used bandwidth.

[0189] Also, f is a view for visually displaying the VPN of the customer to the operation manager as topology. This view f is in practice the VPN fault monitor view utilized for monitoring faults of the VPN.

[0190] Second Embodiment

[0191] Next, an explanation will be made of full automation of VPN service management in the VPN service management system 1 according to the present invention.

[0192] **FIG. 16** is a view of the VPN service management system 1 for explaining a second embodiment (full automation) according to the present invention.

[0193] Note that most of the figure is the same as **FIG. 5**. The difference resides in that the customer network management center (C-NMS) 13 is clearly shown in the customer management center 8. This is for showing that the full automation is achieved by the cooperation of the C-NMS12 and the P-NMS12.

[0194] The point of the second embodiment resides in the following configuration. Namely, the customer network management system (C-NMS) 13 monitors the operation status of the customer network 5 and changes the VPN service conditions by full automation without interposition of an operator through the cooperation of the VPN service agent 3 and both the VPN service manager 2 and the provider network management system (P-NMS) 12 in accordance with the monitoring result.

[0195] More concretely, the VPN service agent 3 has a parameter table for pre-setting and holding changed condition data to be referred to when changing the VPN service conditions. Further, the customer network management system 13 is comprised so as to transmit the changed VPN service conditions determined by referring to the parameter table to the VPN service manager when deciding that the VPN service conditions should be changed due to the monitoring result.

[0196] **FIG. 17** shows a concrete image of the VPN service management system 1 shown in **FIG. 16**.

[0197] Most of the figure is the same as **FIG. 14**. The difference resides in that the parameter table is shown as reference numeral 34, and the VPN service change decision unit 35 referring to the parameter table 34 is shown. The operation is roughly indicated by (1), (2), (3), and (4) in the figure.

[0198] (1) The C-NMS12 first collects the data of the traffic and the service quality of the customer network 5.

[0199] (2) On the other hand, the C-NMS12 retrieves the VPN service conditions given to the concerned customer by referring to the parameter table 34.

[0200] (3) The data collected in the above (1) is compared with the threshold values stored in the parameter table 34. When detecting that the data exceeds any threshold value, an alarm indicating that a threshold value is exceeded is notified to the VPN service change decision unit 35. This is the function of issuing a service order (means 32 of **FIG. 9**).

[0201] (4) When receiving the notification, the VPN service change decision unit 35 refers to the parameter table 34 and transfers the request for change to the VPN service quality capable of covering the amount by which from threshold value is exceeded to the VPN service manager 2 automatically without the interposition of an operator.

[0202] Then the VPN service manager 2 controls the network elements (NE) in the provider network 4 so as to meet that request.

[0203] Concretely summarizing the above, the C-NMS12 manages the conditions concerning the operation status of the customer network 5, for example, the frequency of access through the Internet to the customer network 5 and the rate of flow of traffic to the customer edge (CE). The VPN service agent 3 holds the type of the threshold value, degree of increase, etc. when these conditions exceed a certain threshold value and the VPN service parameter change conditions in the parameter table 34 as the VPN parameters.

[0204] When the C-NMS12 detects that a threshold value of the operation conditions of the customer network 5 has been exceeded, the VPN service agent 3 refers to the parameter table 34, then reflects the changed conditions found into the provider network 4 by the VPN service manager 2 and the P-NMS12. Due to this, it is possible to immediately meet the VPN service conditions in accordance with the operation status of the customer network 5 without the interposition of the operation manager of the customer network 5 and the operation manager of the provider network 4. Here, the parameter table will be simply explained.

[0205] FIG. 18 is a view schematically showing the parameter table 34.

[0206] The content of the table of the top part of the figure is the same as the content of the table 14 shown at the top part of FIG. 7 mentioned above. The VPN service change decision unit 35 decides to change the content of table 34 of the top part of the figure as for example shown in the bottom part of the figure. There are a plurality of levels of decision.

[0207] Level 1 is for when assuming the current value is the value of the "Best Effort" and changes that value to a 20% increase.

[0208] Level 2 is for when the current value is the value of the 20% increase and changes that value to a 50% increase.

[0209] Level 3 is for when the current value is the value of the 50% increase and changes that value to a 100% increase. That is, the higher the level, the broader the changed bandwidth.

[0210] Next, the operation under the above mentioned second embodiment will be explained.

[0211] FIG. 19 is a view of a series of sequences under the second embodiment shown in FIG. 16.

[0212] Assume now that the company receiving the provision of the VPN service suddenly experiences congestion of its network in a certain time band. For this reason, that company desires to rapidly change the VPN service conditions. The change is performed automatically by the following procedure.

[0213] (1) When the C-NMS12 on the customer side judges that the threshold value has been exceeded, the VPN service agent 3 sends an alarm indicating that the traffic threshold value has been exceeded ((1) in the figure).

[0214] The VPN service change decision unit 35 judges that the threshold value of the C-NMS has been exceeded. The judgment logic is installed in the decision unit 35 in advance. The contents thereof are for example as follows.

TABLE 1

Level	Packet loss	Traffic threshold
Level 1	One fault message	Threshold 90%: 5 times
Level 2	Five fault messages	Threshold 90%: 10 times
.	.	.
.	.	.
.	.	.

[0215] (2) The VPN service agent 3 refers to the parameter table 34 ((2) in the figure). Then, it compares this with the present service under that parameter and selects the optimal level of the VPN service conditions.

[0216] (3) When a new VPN service condition is selected, the VPN service agent 3 automatically requests a change to the new VPN service to the VPN service manager 2 ((3) in the figure).

[0217] (4) The VPN service manager 2 receiving the notification of the request reads the current usage bandwidth of the customer and judges whether or not the request for change is possible ((4) in the figure).

[0218] If the change is impossible, the VPN service manager 2 notifies that it is "IMPOSSIBLE" to the VPN service agent 3 of the customer.

[0219] (5) Conversely, when the request for change is "POSSIBLE", the change of service is notified as a command for change of settings of the network elements to the P-NMS12 ((5) in the figure).

[0220] (6) The P-NMS12 issues a command for change of settings of the network elements, for example, a policy setting, to the network elements (NE) on the provider side according to the conditions indicated in the parameter table 34. By this, the VPN service contents of the company side are changed. According to this example, the bandwidth of the network becomes broader, so the congestion and the packet loss are automatically solved and suppressed ((6) in the figure).

[0221] (7) When the settings of the network elements (NE) are successfully changed, the success is notified to the P-NMS12 ((7) in the figure).

[0222] (8) When succeeding in changing to the new service by the above description, the P-NMS12 sends a reply to this effect to the VPN service manager 2 ((8) in the figure).

[0223] (9) The VPN service manager 2 notifies the change to the VPN service agent 3 on the customer side by utilizing the concerned VPN service ((9) in the figure).

[0224] (10) When the change to new service is notified, the VPN service agent 3 records the parameters of the present service in the database (database for storing the parameter table 34) ((10) in the figure).

[0225] As described above, by increasing the VPN service bandwidth for a certain period, congestion of the network can be automatically dealt with.

[0226] Third Embodiment

[0227] Next, an explanation will be made of semi-automation of VPN service management in the VPN service management system according to the present invention.

[0228] **FIG. 20** is a view of the VPN service management system **1** for explaining a third embodiment (semi-automation) according to the present invention.

[0229] Note that most of the figure is the same as **FIG. 16**. The difference resides in that a client terminal **41** placed inside the customer management center **8** and a remote client terminal **42** located at a remote place are shown and that an operation status change notifying means **43** is shown. Note that, the client terminals **41** and **42** will also be referred to overall as an operation manager **(40)**.

[0230] The point of the third embodiment resides in the following configuration. Namely, an operation status change notifying means **43** is provided in the VPN service agent **3**, when, the customer network management system (C-NMS) 13 monitors the operation status of the customer network **5** and decides that the VPN service conditions should be changed by the monitor result, for notifying the decision to the operation manager **40** of the customer network **5**, and this VPN service agent **3** semi-automatically changes the VPN service conditions through cooperation of the VPN service manager **2** and the provider network management system (P-NMS) 12 when receiving a reply giving permission with respect to the notification.

[0231] Further concretely, the VPN service agent **3** has a parameter table **34** (refer to **FIG. 17**) for pre-setting and holding the changed condition data to be referred to when changing the VPN service conditions. When the customer network management system (C-NMS) 13 judges by the monitoring result that the VPN service conditions should be changed, the changed VPN service conditions determined by referring to the parameter table **34** are input to the operation status change notifying means **43**.

[0232] Note that the view of the concrete image of the VPN service management system **1** based on the third embodiment is almost the same as the above mentioned **FIG. 17**, so is omitted, but the concrete image of the system **1** may be summarized as follows.

[0233] The VPN service agent **3** has an operation status change notifying means **43** for notifying the above mentioned type of threshold value, degree of increase, etc. and the conditions for change of the VPN service parameters together with the VPN parameter table **34** (refer to **FIG. 18**) to the operation manager **40** of the customer network **5**.

[0234] When the C-NMS12 detects that a threshold value of the operation conditions of the customer network **5** has been exceeded, the VPN service agent **3** refers to the parameter table **34**, then notifies the fact that it has been exceeded to the operation manager **40**. Then, the judgment of the operation manager **40** is reflected in the provider network **4** by using the VPN service manager **2** and the P-NMS12. By this, VPN service conditions in accordance with the operation status of the customer network **5** can be promptly met under the judgment of the operation manager **4** without the interposition of the operator of the provider network **4**.

[0235] **FIG. 21** is a view of a series of sequences under the third embodiment shown in **FIG. 20**.

[0236] The figure is similar to the sequence diagram of **FIG. 19**. Processes similar to each other are indicated by the same numerals in parentheses.

[0237] When assuming that a company receiving provision of a VPN service suddenly experiences congestion of the network in a certain time band, the following processes (1), (2), . . . are proceeded with in the following sequence. Note that (11), (12), etc. are processes distinctive to the third embodiment.

[0238] (1) Same as (1) of **FIG. 19**.

[0239] (2) Same as (2) of **FIG. 19**.

[0240] (11) The service level (refer to the bottom part of **FIG. 18**) selected by the VPN service agent **3** is notified to the operation manager **4** ((11) in the figure).

[0241] (12) The operation manager **40** judges whether or not this new service level is to be applied to the concerned company and sends back the result of judgment to the VPN service agent **3** ((12) in the figure).

[0242] (3) The VPN service agent **3** notified of the result of judgment for the request of change automatically requests the result, as the new VPN service change demand, to the VPN service manager **2**.

[0243] (4) to (9) are same as (4) to (9) of **FIG. 19**.

[0244] (13) The setting of the VPN service conditions was changed by the above, so this is reflected in the C-NMS12. In the case of semi-automation, unlike the case of full automation mentioned above, the final result cannot be confirmed by the C-NMS12, so this process (13) is necessary.

[0245] As described above, by increasing the VPN service bandwidth for a certain period, congestion of the network can be semi-automatically handled.

[0246] As mentioned above, in a semi-automation VPN service, when notified that a threshold value has been exceeded or is predicted to be exceeded based on the parameter table **34** set in advance, the VPN service change decision unit **35** (refer to **FIG. 17**) refers to the service conditions of the parameter table **34** and automatically decide what kind of service should be selected. At this time, that decision is input to the notifying means **43**. Based on the concerned input, the operation manager **40** (operator) finally reconfirms the result of the decision by the service change decision unit **35**. When there is no problem in the change of the service content, the operator requests the change of the service content to the VPN service manager **2** of the provider network **4**.

[0247] Thus, the VPN service conditions in accordance with the operation status of the customer network **5** can be promptly met without the interposition of the operation manager of the provider network **4**.

[0248] Fourth Embodiment

[0249] Next, an explanation will be made of server/client type management in the VPN service management system **1** according to the present invention.

[0250] **FIG. 22** is a view of the VPN service management system **1** for explaining the fourth embodiment (server/client type) according to the present invention.

[0251] Note, most of the figure is the same as **FIG. 20**. The difference resides in that the operation status change notifying means **43** is realized by a server/client mode.

[0252] The point of the fourth embodiment resides in the following configuration. Namely, when the VPN service agent **3** and the customer network management system (P-NMS) **13** cooperate in a server/client mode, the remote client terminal **42** attached to the operation manager **40** is introduced as another one of the concerned clients. Further, the VPN service agent **3** and the remote client terminal **42** cooperate in a server/client mode to realize the operation status change notifying means **43**.

[0253] The VPN service agent **3** and the remote client terminal **42** are more preferably connected by a leased line or in-band.

[0254] **FIG. 23** is a view of a concrete image of the VPN service management system **1** shown in **FIG. 22**.

[0255] Most of the figure is the same as **FIG. 17**. The difference resides in that the operation status change notifying means **43** mentioned above is shown as the VPN service change notification unit **44**. Also, among (1), (2), (3), and (4) representing operations, the operation (3) is different. In the fourth embodiment, in this (3), the VPN service change notification unit **44** receives a notification of a change of the VPN service parameters from the C-NMS12 side.

[0256] Summarizing the configurations of **FIG. 22** and **FIG. 23**, the operation status change notifying means **43** can be realized as an alarm displaying means on the operation terminals (**41, 42**) operated with the C-NMS12 and the VPN service agent **3**. There is a terminal at a place other than the customer network management center **8**. This is connected to the VPN service agent **3** as the remote client terminal **42**.

[0257] In the case of remote operation, the operation manager terminals (**41, 42**) and the VPN service agent **3** operate in a server and client relationship and are connected to each other by a corporate LAN or in-band.

[0258] **FIG. 24** is a view of the series of sequences under the fourth embodiment shown in **FIG. 22**.

[0259] The figure is almost the same as the sequence diagram of **FIG. 21**. Similar processes are indicated by the same numerals in parentheses. The particularly different point resides in that the VPN service agent **3** and the terminals (**41, 42**) of the operation manager **40** are represented in a server/client mode in the top part of **FIG. 24**.

[0260] Accordingly, the processes (1) to (13) of the figure are the same as the processes (1) to (13) of **FIG. 21**, but this is different from the third embodiment in the point of the VPN service by remote operation.

[0261] In this VPN service, the person responsible for the operation of the customer network **5** (president, operator, etc.) can ask for a request for change of service to the provider side by the remote client **42** from time to time. The remote client **42** is connected to the service agent **3** of the customer network **5** and determines the service conditions in the parameter table **34** by the judgment of the person responsible for operation of the customer network **4**. Based on the result, the service agent **3** side requests the service contents to the VPN service manager **2** of the provider network **4**. The remote client **42** is connected to the service agent **3** of the customer network **5** by a leased line or in-band, so there is no problem in security.

[0262] Also, by the remote operation, the operation manager **40** can manage the VPN not only at a fixed location, but also at a remote location. As described above, by increasing the VPN service bandwidth for a certain period, congestion of the network can be dealt with by remote operation.

[0263] Fifth Embodiment

[0264] Next, an explanation will be made of remote permission response type of management in the VPN service management system **1** according to the present invention.

[0265] **FIG. 25** is a view of the VPN service management system **1** for explaining the fifth embodiment (remote permission response type) according to the present invention.

[0266] Note that most of the figure is the same as **FIG. 16** mentioned above. The difference resides in that, as an example, a radio area network (RAN) **51** and a mobile terminal **52** are shown.

[0267] The point of the fifth embodiment resides in the following configuration. Namely, an operation status change confirming means **53** is provided in the VPN service manager **2** side, when the customer network management system (C-NMS) **13** monitors the operation status of the customer network **5**, for requesting confirmation to the customer, that is, the remote operation manager **40**, upon receipt of a request to the VPN service manager **2** for automatically changing of the VPN service conditions in accordance with the monitoring result, and the VPN service manager **2** changes the VPN service conditions when obtaining a reply of permission with respect to the notification.

[0268] More concretely, the operation status change confirming means **53** is realized by the VPN service manager **2** and the mobile terminal **52** wirelessly connected to the provider network.

[0269] In this case, as mentioned above, the VPN service agent **3** has a parameter table **34** for pre-setting and holding the changed condition data which should be referred to when changing the VPN service condition. The customer network management system **13** transmits the changed VPN service conditions determined by referring to the parameter table **34** to the VPN service manager **2** when judging that the VPN service condition should be changed according to the monitoring result.

[0270] **FIG. 26** is a view of a series of sequences under the fifth embodiment shown in **FIG. 25**.

[0271] The figure is similar to the sequence diagram of **FIG. 21**. Similar processes are indicated by the same numerals in parentheses. The particular difference resides in that the mobile terminal **52** and the operation status confirming means **53** are represented at the top part of **FIG. 26**.

Also, when looking at the process, the notification process (11) of **FIG. 21** becomes the notification process (21) extended to the VPN service manager **2** in **FIG. 26**, the process (22) for confirmation of a request for change made via the process (21) is added to the operation manager (mobile terminal) **52**, and the process (23) for returning a reply for permission obtained by that confirmation from the mobile terminal **52** to the manager **2** is added.

[0272] Summarizing the configurations of **FIG. 25** and **FIG. 26**, in the VPN service, the operation status change confirming means **53** is made able to use the Internet mail or the portable telephone (**52**) to change the VPN service conditions from a location other than the operation management center **8** of the customer network **5** as well. That is, there is a mobile terminal **52** in addition to the customer network management center **8**. The VPN service is controlled semi-automatically by remote operation.

[0273] Information is sent to the mobile terminal **52** (customer operation manager) via the RAN **51** of the provider network **4**. Note that the method of connection to the customer operation manager (**52**) for confirmation as in the embodiment described above is as follows.

[0274] **FIG. 27** is a view schematically showing the method of connection to the operation manager, while **FIG. 28** is a view schematically showing advance preparations with the operation manager.

[0275] According to **FIG. 27**, the terminal **41** of the operation manager **40** selects the method of connection (communication means) in advance.

[0276] Next, the mail address (Mail) of the destination or the number of the portable telephone (Mobile) is input.

[0277] Referring to **FIG. 28**, the content of the mail sent to the mobile terminal **52** is illustrated.

[0278] As the above advance preparations, it is necessary to set the contract contents of the VPN service conditions. An example of the contents is shown in **FIG. 28**.

[0279] When performing the control at the mobile terminal **52**, the contract contents are set in advance as the advance preparations for simplifying the operation at the mobile terminal **52**. This makes it possible for the owner of the terminal **52** to easily respond. For example, he or she may press the # key to input the number. The terminal **52** may be notified by voice or mail.

[0280] Thus, the operation manager **40** can dynamically change the VPN service conditions by the selection of the mail address or the number of the mobile terminal. Even if the manager of the customer network **5** is absent, there is no influence upon the VPN service of the customer.

[0281] That is, even if the customer side operation manager **40** is not in the network management center **8**, it is possible to set the VPN service conditions, for example, increase the VPN service bandwidth.

[0282] Sixth Embodiment

[0283] Next, an explanation will be made of a mode of communication between the manager and an agent in the VPN service management system **1** according to the present invention.

[0284] **FIG. 29** is a view of the configuration of **FIG. 17** with the sixth embodiment applied thereto.

[0285] Accordingly, most of the figure is the same as the configuration of **FIG. 17**. The difference resides in that a customer side in-band means **61** and a provider side in-band means **62** are shown.

[0286] The point of the sixth embodiment resides in the following configuration. Namely, in-band means for using the VPN per se, as in-band, constructed by a contract between the provider and the customer is provided for cooperation between the VPN service manager **2** and the VPN service agent **3**.

[0287] Concretely, the in-band means **61** and **62** are formed as illustrated by reference numerals **61** and **62** at the customer edge (CE) and the provider edge (PE) arranged inside the provider network **4** for connection with the customer edge (CE).

[0288] Since the in-band is utilized in this way, the operation of (4) ("VPN service condition change order") in **FIG. 17** is carried out through the route **63** in-band as shown in **FIG. 29**.

[0289] Summarizing this, according to the sixth embodiment, by using the VPN per se contracted for between the provider and the customer in-band as the communication means between the VPN service agent **3** and the VPN service manager **2**, a change of the VPN service conditions can be communicated without introducing a new independent communication means. Also, security can be simultaneously maintained.

[0290] Next, the in-band means will be explained.

[0291] **FIG. 30** is a view explaining the in-band means according to the present invention.

[0292] In the figure, the customer edge (CE) is provided with a mechanism (in-band means **61**) for transferring information at the monitor use port by VPN in-band.

[0293] Similarly, the provider edge (PE) is provided with a mechanism (in-band means **62**) for transferring the information at the monitor use port by VPN in-band.

[0294] In order to realize the mechanism necessary for this provider edge, the following two information (i) and (ii) are set in advance as configuration data on the provider edge PE:

[0295] (i) IP address of the VPN service agent **3** managing the concerned provider edge (PE).

[0296] (ii) Identifier (VPN-id) of VPN through which the information should pass between the customer and the provider.

[0297] On the other hand, in order to realize the mechanism necessary for the customer edge (CE), the method of connection of the customer edge (CE) and the VPN service agent **3** must be considered. Two plans of this method of connection are shown in the figure.

[0298] **FIG. 31** is a view of a first connection method between the customer edge (CE) and the agent **3**, while **FIG. 32** is a view of a second connection method between the customer edge (CE) and the agent **3**.

[0299] FIG. 31 shows a method of directly connecting the customer edge (CE) from the maintenance terminal use Ethernet port on the customer edge (CE) side to the agent 3 without via the network.

[0300] FIG. 32 shows a method of connecting the customer edge (CE) and the agent 3 via the network (customer network 5).

[0301] FIG. 33 is a view of an example of connection between the manager 2 and the agent 3 under the in-band mode.

[0302] This will be explained according to the figures.

[0303] (1) The control information reaches up to the customer edge (CE) of the concerned VPN (customer A network) by the above (ii), that is, VPN-id. Next, (2) the control information departs for the network (customer A network) side by either of the above two connection methods (FIG. 31, FIG. 32), then (3) the control information reaches the VPN service agent A(3-A) of the intended IP address by the above (i), that is, the IP address.

[0304] Note that, for the communication means between the provider edge (PE) and the VPN service manager 2, there are known techniques such as the method of setting an independent VPN network and the method of leasing an existing VPN from the provider edge (PE) to the middle and utilizing the IP network between the middle and the VPN service manager 2.

[0305] While the overall VPN service management system 1 according to the present invention was explained in detail above, the characteristic feature of the present invention resides in not only the system 1 as a whole, but also the VPN service manager 2 per se and the VPN service agent 3 per se comprising that system 1. The characteristic configuration of the VPN service manager 2 per se and the characteristic configuration of the VPN service agent 3 will be summarized on the basis of the explanation based on FIG. 1 to FIG. 30 mentioned above.

[0306] First, the characteristic configuration of the VPN service manager 2 per se is as follows.

[0307] (A) The VPN service manager 2 is a VPN service manager comprising part of a VPN service management system 1 for managing a VPN service for a communication network provided with a customer network 5 servicing customers and a provider network 4 constructed by a provider for providing the VPN service to the customers and connected to the customer network 5.

[0308] This manager 2 is comprised so as to manage the VPN service for the provider network 4 and to change the VPN service conditions of the VPN service to be provided by the VPN service management system 1 in real time in accordance with the operation status of the customer network 5 under the management of the VPN service agent 3 in cooperation with the VPN service agent 3 managing the VPN service for the customer network 5.

[0309] Further, this manager 2 is comprised of a VPN service order control means 21 for receiving an order for changing a VPN service condition when the order is generated from the VPN service agent 3 and outputting the changed VPN service condition related to that order, a VPN service condition retrieval means 22 for retrieving a present VPN service condition given to the concerned customer network 5 from the VPN service condition table 14 when that order is generated, a VPN service condition decision means 23 for deciding whether or not a range by which the changed VPN service condition exceeds the present VPN service condition is within an allowable range, a VPN service condition setting means 24 for resetting the present VPN service condition to the changed VPN service condition when the result of the decision is "POSSIBLE", and a customer edge control means 25 for controlling a customer edge (CE) based on the reset VPN service condition.

[0310] Here, the manager 2 has an operation status change notifying means 43 for notifying an operation manager 40 of the customer network 5 of a request for change of a VPN service condition from the customer network management system 13 automatically in accordance with a monitoring result when a customer network management system (C-NMS) 13 monitors the operation status of the customer network 5 and changes the VPN service condition when obtaining a reply of permission with respect to the notification.

[0311] (B) On the other hand, the VPN service agent 3 is a VPN service agent comprising part of a VPN service management system 1 for managing a VPN service for a communication network provided with a customer network 5 servicing customers and a provider network 4 constructed by a provider for providing the VPN service to the customers and connected to the customer network 5.

[0312] This agent 3 is comprised so as to manage the VPN service for the customer network 5 and to change a VPN service condition of the VPN service to be provided by the VPN service management system 1 in real time in accordance with the operation status of the customer network 5 under management in cooperation with a VPN service manager 2 managing a VPN service for a provider network 4.

[0313] Further, this agent 3 has a customer network management system (C-NMS) 13 for managing the customer network 5. This customer network management system 13 monitors the customer edge (CE) and communicates with the provider network 4 side.

[0314] Further, this agent 3 is provided with a service menu concerning the VPN service from the VPN service manager 2 as a VPN service condition table 14 and transmits a request for change via the service menu to the VPN service manager 2 when a request for change of a VPN service condition is generated at the customer side.

[0315] Also, this agent 3 is provided with a VPN service condition retrieval means 31 for retrieving a current VPN service condition given to the concerned customer network 5 from the VPN service condition table 14 when an order for changing a VPN service condition is generated from the customer and a VPN service order issuing means 32 for issuing an order to the VPN service manager 2 based on the retrieved VPN service condition.

[0316] Further, this agent 3 has a parameter table 34 for pre-setting and holding changed condition data to be referred to when changing a VPN service condition. The customer network management system (C-NMS) 13 trans-

mits the changed VPN service condition determined by referring to the parameter table **34** to the VPN service manager **2** when deciding that the VPN service condition should be changed by the monitoring result.

[0317] Furthermore, this agent **3** has an operation status change notifying means **43** for notifying a decision to an operation manager **40** of the customer network **5** when the customer network management system **13** monitors the operation status of the customer network **5** and decides that a VPN service condition should be changed by the monitoring result and changes the VPN service condition by cooperation of the VPN service manager **2** and a provider network management system (P-NMS) **12** when obtaining a reply of permission with respect to the notification.

[0318] As explained in detail above, according to the present invention, in a VPN service, the following effects can be obtained.

[0319] 1) A request on the customer side that the contract conditions between the customer and the provider be changed can be rapidly responded to.

[0320] 2) The quality conditions and usage conditions of a VPN service such as an IP-VPN service can be easily changed.

[0321] 3) The service level agreement contracted for between a customer and the provider can be always fulfilled.

[0322] While the invention has been described with reference to specific embodiments chosen for purpose of illustration, it should be apparent that numerous modifications could be made thereto by those skilled in the art without departing from the basic concept and scope of the invention.

What is claimed is:

1. A VPN service management system for managing a VPN service for a communication network provided with a customer network for servicing customers and a provider network constructed by a provider for providing the VPN service to the customers and connected to the customer network, comprising:

a VPN service manager for managing said VPN service for said provider network; and

a VPN service agent for managing said VPN service for said customer network,

said VPN service manager changing a VPN service condition of said VPN service to be provided in real time in accordance with an operation status of said customer network under the management of the VPN service agent in cooperation with said VPN service agent.

2. A VPN service management system as set forth in claim 1,

said system further comprising a provider network management system cooperating with said VPN service manager on said provider side,

said provider network management system managing the provider network including also a customer edge arranged in said customer network for connection with said provider network.

3. A VPN service management system as set forth in claim 2,

said system further comprising a customer network management system cooperating with said VPN service agent and managing said customer network on said customer side,

the customer network management system monitoring said customer edge and communicating with said provider network side.

4. A VPN service management system as set forth in claim 2, wherein

said VPN service manager provides a service menu concerning the VPN service as a VPN service condition table to said VPN service agent,

when there is a request for change of a VPN service condition on said customer side, the VPN service agent transmits the request for change to the VPN service manager via said service menu, and

the VPN service manager reflects the request for change in said provider network via said provider network management system.

5. A VPN service management system as set forth in claim 1, wherein said VPN service manager is comprised of:

a VPN service order control means for receiving an order when an order for changing the VPN service conditions is generated from a VPN service agent and outputting the changed VPN service conditions concerned in that order,

a VPN service condition retrieval means for retrieving the present VPN service conditions given to the concerned customer network from the VPN service condition table when that order is generated,

a VPN service condition decision means for deciding whether or not the range by which the changed VPN service conditions exceed the present VPN service conditions is within an allowable range,

a VPN service condition setting means for resetting the present VPN service conditions to the changed VPN service conditions when the result of said decision is "POSSIBLE", and

a customer edge control means for controlling the customer edge based on the reset VPN service-conditions.

6. A VPN service management system as set forth in claim 1, wherein said VPN service agent is comprised of:

a VPN service condition retrieval means for retrieving a current VPN service condition given to the customer network from the VPN service condition table when an order for changing the VPN service conditions is generated from a customer; and

a VPN service order issuing means for issuing the order to the VPN service manager based on the retrieved VPN service condition.

7. A VPN service management system as set forth in claim 6, wherein the VPN service manager is provided with a customer edge control means for controlling a customer edge based on the VPN service condition reset by the VPN

service manager upon receipt of said order when said VPN service manager controls the customer edge through said VPN service agent.

8. A VPN service management system as set forth in claim 3, wherein said customer network management system monitors the operation status of said customer network and changes of said VPN service condition by full automation without interposition of an operator through cooperation of said VPN service agent and both said VPN service manager and said provider network management system in accordance with the monitoring result.

9. A VPN service management system as set forth in claim 8, wherein

said VPN service agent has a parameter table for presetting and holding changed condition data to be referred to when changing said VPN service condition, and

said customer network management system transmits the changed VPN service condition determined by referring to said parameter table to said VPN service manager when deciding that said VPN service condition should be changed by said monitoring result.

10. A VPN service management system as set forth in claim 3, wherein

said system provides in said VPN service agent an operation status change notifying means for notifying a decision to an operation manager of said customer network when said customer network management system monitors the operation status of said customer network and decides that said VPN service condition should be changed by the monitoring result and

the VPN service agent semi-automatically changes said VPN service condition by cooperation of said VPN service manager and said provider network management system when obtaining a reply of permission with respect to said notification.

11. A VPN service management system as set forth in claim 10, wherein

said VPN service agent has a parameter table for presetting and holding changed condition data to be referred to when changing said VPN service condition and

inputs the changed VPN service condition determined by referring to said parameter table to said operation status change notifying means when said customer network management system judges by said monitoring result that said VPN service condition should be changed.

12. A VPN service management system as set forth in claim 10, wherein,

when said VPN service agent and said customer network management system cooperate in a server/client mode, a remote client terminal attached to said operation manager is introduced as another one of the clients, and

said operation status change notifying mean is realized by cooperation of said VPN service agent and said remote client terminal in the server/client mode.

13. A VPN service management system as set forth in claim 12, wherein said VPN service agent and said remote client terminal are connected by a leased line or in-band.

14. A VPN service management system as set forth in claim 3,

said system providing at said VPN service manager side an operation status change confirming means for requesting confirmation at a remote operation manager of a customer upon receipt of a request when said customer network management system monitors the operation status of said customer network and automatically request a change of said VPN service condition to said VPN service manager in accordance with the monitoring result and

said VPN service manager changes said VPN service condition when obtaining a reply of permission with respect to said notification.

15. A VPN service management system as set forth in claim 14, wherein said operation status change confirming means is realized by said VPN service manager and a mobile terminal wirelessly connected to said provider network.

16. A VPN service management system as set forth in claim 14, wherein

said VPN service agent has a parameter table for presetting and holding changed condition data to be referred to when changing said VPN service condition, and

said customer network management system transmits the changed VPN service condition determined by referring to said parameter table to said VPN service manager when judging that said VPN service condition should be changed according to said monitoring result.

17. A VPN service management system as set forth in claim 3, further having an in-band means for using the VPN per se, as in-band, constructed by a contract between said provider and said customer in-band for said cooperation between said VPN service manager and said VPN service agent.

18. A VPN service management system as set forth in claim 17, wherein in-band means are formed at said customer edge and a provider edge arranged inside said provider network for connection with the customer edge.

19. A VPN service manager comprising part of a VPN service management system for managing a VPN service for a communication network provided with a customer network servicing customers and a provider network constructed by a provider for providing the VPN service to the customers and connected to the customer network,

said VPN service manager is operative to manage the VPN service for the provider network and

change a VPN service condition of the VPN service to be provided by the VPN service management system in real time in accordance with the operation status of the customer network under the management of a VPN service agent managing the VPN service for the customer network in cooperation with the VPN service agent.

20. A VPN service manager as set forth in claim 19, provided with:

a VPN service order control means for receiving an order for changing a VPN service condition when the order is generated from the VPN service agent and outputting the changed VPN service condition related to that order,

a VPN service condition retrieval means for retrieving a present VPN service condition given to the concerned customer network from the VPN service condition table when that order is generated,

a VPN service condition decision means for deciding whether or not a range by which the changed VPN service condition exceeds the present VPN service condition is within an allowable range,

a VPN service condition setting means for resetting the present VPN service condition to the changed VPN service condition when the result of the decision is "POSSIBLE", and

a customer edge control means for controlling a customer edge based on the reset VPN service condition.

21. A VPN service manager as set forth in claim 19, further

having an operation status change notifying means for notifying an operation manager of the customer network of a request for change of a VPN service condition from the customer network management system automatically in accordance with a monitoring result when a customer network management system monitors the operation status of the customer network and

changing the VPN service condition when obtaining a reply of permission with respect to the notification.

22. A VPN service agent comprising part of a VPN service management system for managing a VPN service for a communication network provided with a customer network servicing customers and a provider network constructed by a provider for providing the VPN service to the customers and connected to the customer network,

said VPN service agent is operative to manage the VPN service for the customer network and

change a VPN service condition of the VPN service to be provided by the VPN service management system in real time in accordance with the operation status of the customer network under management in cooperation with a VPN service manager managing a VPN service for a provider network.

23. A VPN service agent as set forth in claim 22, wherein

the agent has a customer network management system for managing the customer network and

this customer network management system monitors a customer edge and communicates with the provider network side.

24. A VPN service agent as set forth in claim 22, which

is provided with a service menu concerning the VPN service from the VPN service manager as a VPN service condition table and

transmits a request for change via the service menu to the VPN service manager when a request for change of a VPN service condition is generated at the customer side.

25. A VPN service agent as set forth in claim 22, further provided with:

a VPN service condition retrieval means for retrieving a current VPN service condition given to the concerned customer network from the VPN service condition table when an order for changing a VPN service condition is generated from the customer and

a VPN service order issuing means for issuing an order to the VPN service manager based on the retrieved VPN service condition.

26. A VPN service agent as set forth in claim 23, wherein

the agent has a parameter table for pre-setting and holding changed condition data to be referred to when changing a VPN service condition and

the customer network management system transmits the changed VPN service condition determined by referring to the parameter table to the VPN service manager when deciding that the VPN service condition should be changed by the monitoring result.

27. A VPN service agent as set forth in claim 23, wherein

the agent has an operation status change notifying means for notifying a decision to an operation manager of the customer network when the customer network management system monitors the operation status of the customer network and decides that a VPN service condition should be changed by the monitoring result and

changes the VPN service condition by cooperation of the VPN service manager and a provider network management system when obtaining a reply of permission with respect to the notification.

* * * * *

US 20010027484A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2001/0027484 A1

(43) Pub. Date: Oct. 4, 2001

(Document 1)

Nishi

(54) QUALITY ASSURED NETWORK SERVICE PROVISION SYSTEM COMPATIBLE WITH A MULTI-DOMAIN NETWORK AND SERVICE PROVISION METHOD AND SERVICE BROKER DEVICE

(75) Inventor: Koji Nishi, Tokyo (JP)

Correspondence Address:
OSTROLENK FABER GERB & SOFFEN
1180 AVENUE OF THE AMERICAS
NEW YORK, NY 100368403

(73) Assignee: NEC Corporation

(21) Appl. No.: 09/818,955

(22) Filed: Mar. 27, 2001

(30) Foreign Application Priority Data

Mar. 30, 2000 (JP) 2000-095393

Publication Classification

(51) Int. Cl.[7] G06F 15/173; G06F 15/16

(52) U.S. Cl. 709/223; 709/235

(57) ABSTRACT

The invention provides quality assured network services in a multi-domain network and comprises a network service management device for managing device clusters incorporated within the operations management network of each provider network and receiving service orders, and a multi-domain service broker for providing a broker function for achieving agreement between a plurality of providers, and the multi-domain service broker *further* comprises a device for collecting domain information and information relating to the services each provider is able to provide from the network service management devices, and a device which on receipt of a network service request from a customer, extracts the network service management device of the domain which is able to satisfy the required quality level, and then issues instructions for the setting of the required information within the extracted network service management device.

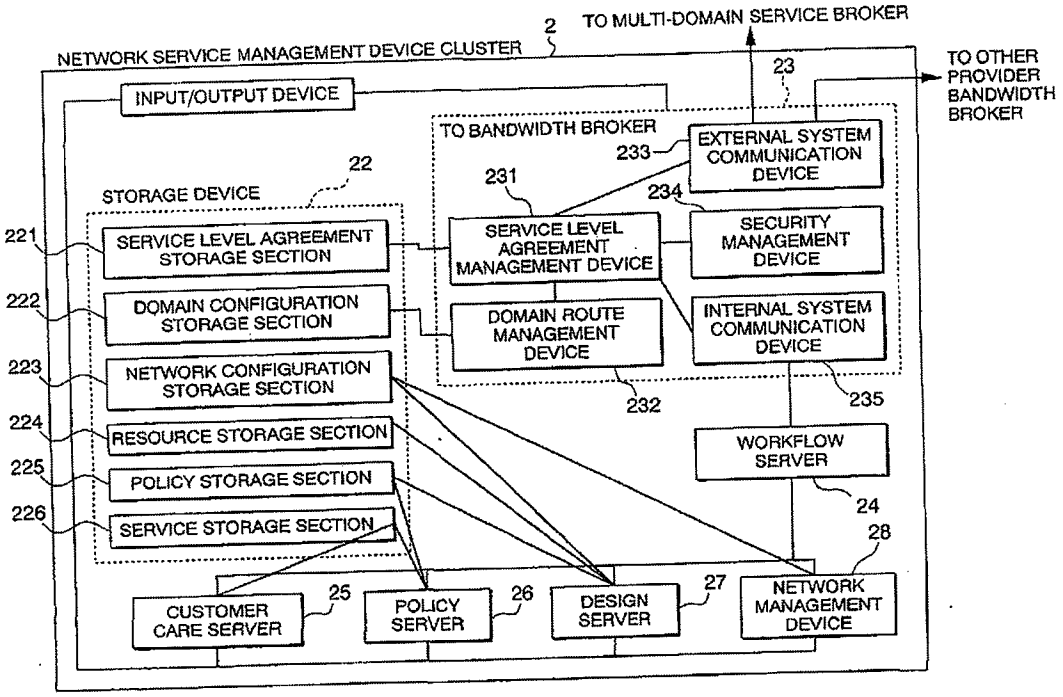


Fig. 1

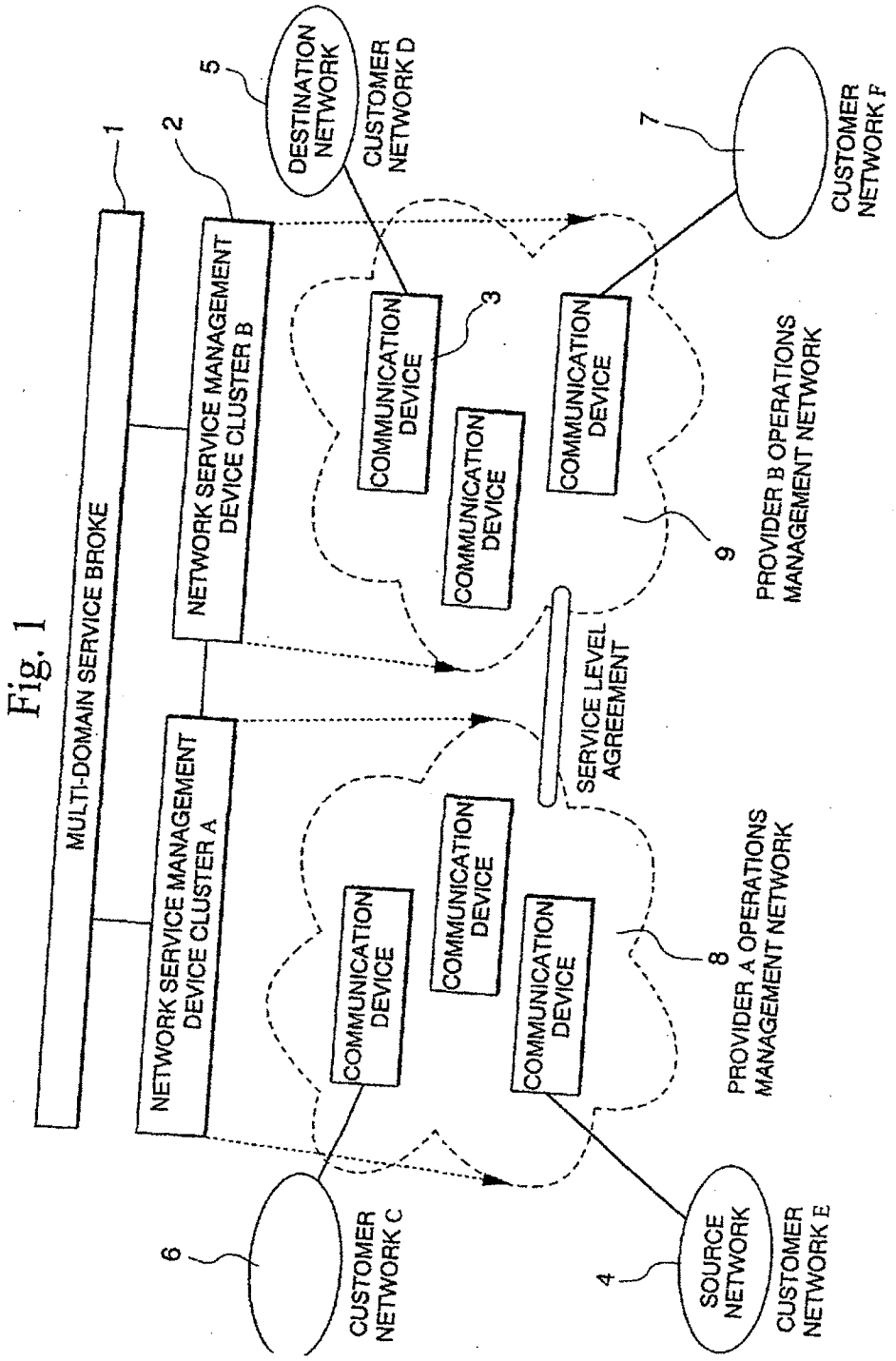

MULTI-DOMAIN SERVICE BROKE
1
NETWORK SERVICE MANAGEMENT DEVICE CLUSTER A
NETWORK SERVICE MANAGEMENT DEVICE CLUSTER B
2
DESTINATION NETWORK
CUSTOMER NETWORK D
5
CUSTOMER NETWORK F
7
COMMUNICATION DEVICE
3
COMMUNICATION DEVICE
COMMUNICATION DEVICE
COMMUNICATION DEVICE
COMMUNICATION DEVICE
COMMUNICATION DEVICE
SERVICE LEVEL AGREEMENT
9
PROVIDER B OPERATIONS MANAGEMENT NETWORK
8
PROVIDER A OPERATIONS MANAGEMENT NETWORK
6
CUSTOMER NETWORK C
4
SOURCE NETWORK
CUSTOMER NETWORK E

Fig. 2

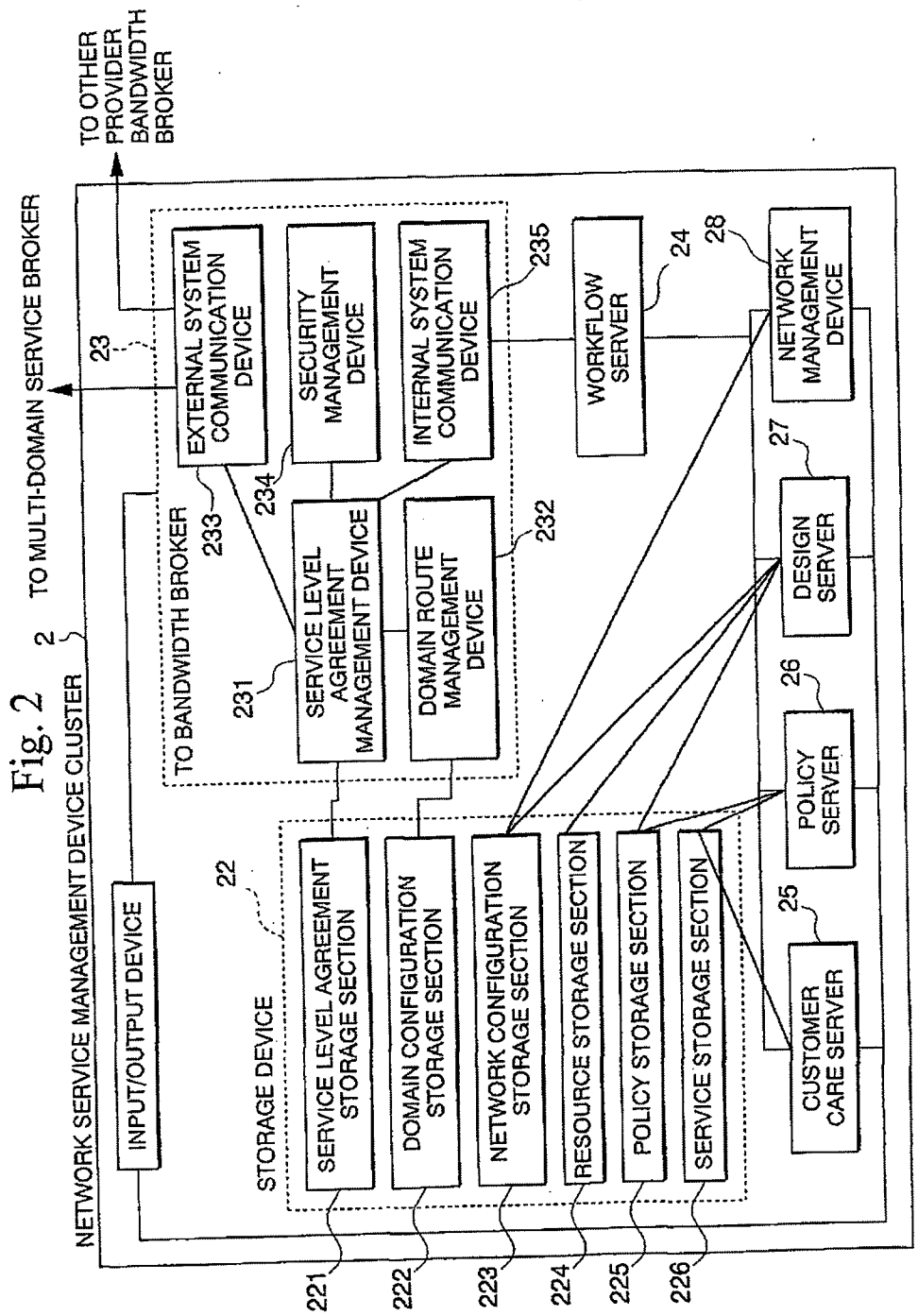

NETWORK SERVICE MANAGEMENT DEVICE CLUSTER
2
TO MULTI-DOMAIN SERVICE BROKER
TO OTHER PROVIDER BANDWIDTH BROKER
23
INPUT/OUTPUT DEVICE
TO BANDWIDTH BROKER
EXTERNAL SYSTEM COMMUNICATION DEVICE
233
SECURITY MANAGEMENT DEVICE
234
INTERNAL SYSTEM COMMUNICATION DEVICE
235
WORKFLOW SERVER
24
28
NETWORK MANAGEMENT DEVICE
231
SERVICE LEVEL AGREEMENT MANAGEMENT DEVICE
DOMAIN ROUTE MANAGEMENT DEVICE
232
27
DESIGN SERVER
26
POLICY SERVER
22
STORAGE DEVICE
SERVICE LEVEL AGREEMENT STORAGE SECTION
DOMAIN CONFIGURATION STORAGE SECTION
NETWORK CONFIGURATION STORAGE SECTION
RESOURCE STORAGE SECTION
POLICY STORAGE SECTION
SERVICE STORAGE SECTION
25
CUSTOMER CARE SERVER
221
222
223
224
225
226

Fig. 3

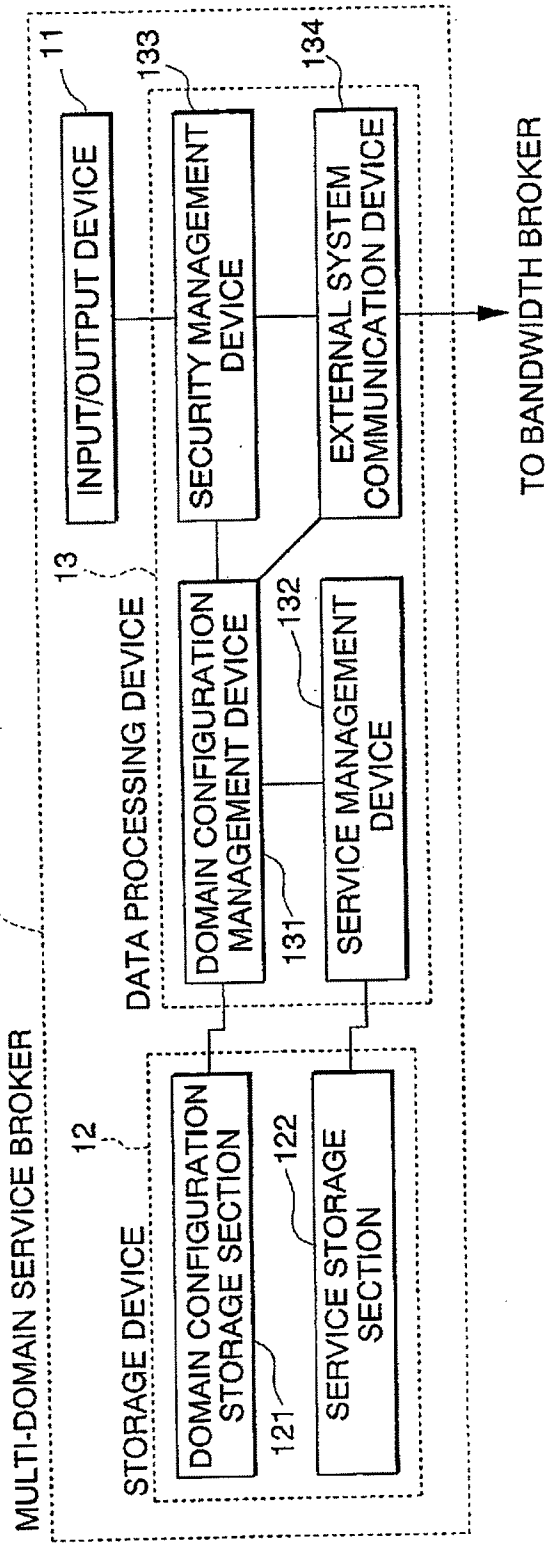

1
MULTI-DOMAIN SERVICE BROKER
11
INPUT/OUTPUT DEVICE
12
STORAGE DEVICE
121
DOMAIN CONFIGURATION STORAGE SECTION
122
SERVICE STORAGE SECTION
13
DATA PROCESSING DEVICE
131
DOMAIN CONFIGURATION MANAGEMENT DEVICE
132
SERVICE MANAGEMENT DEVICE
133
SECURITY MANAGEMENT DEVICE
134
EXTERNAL SYSTEM COMMUNICATION DEVICE
TO BANDWIDTH BROKER

Fig. 4

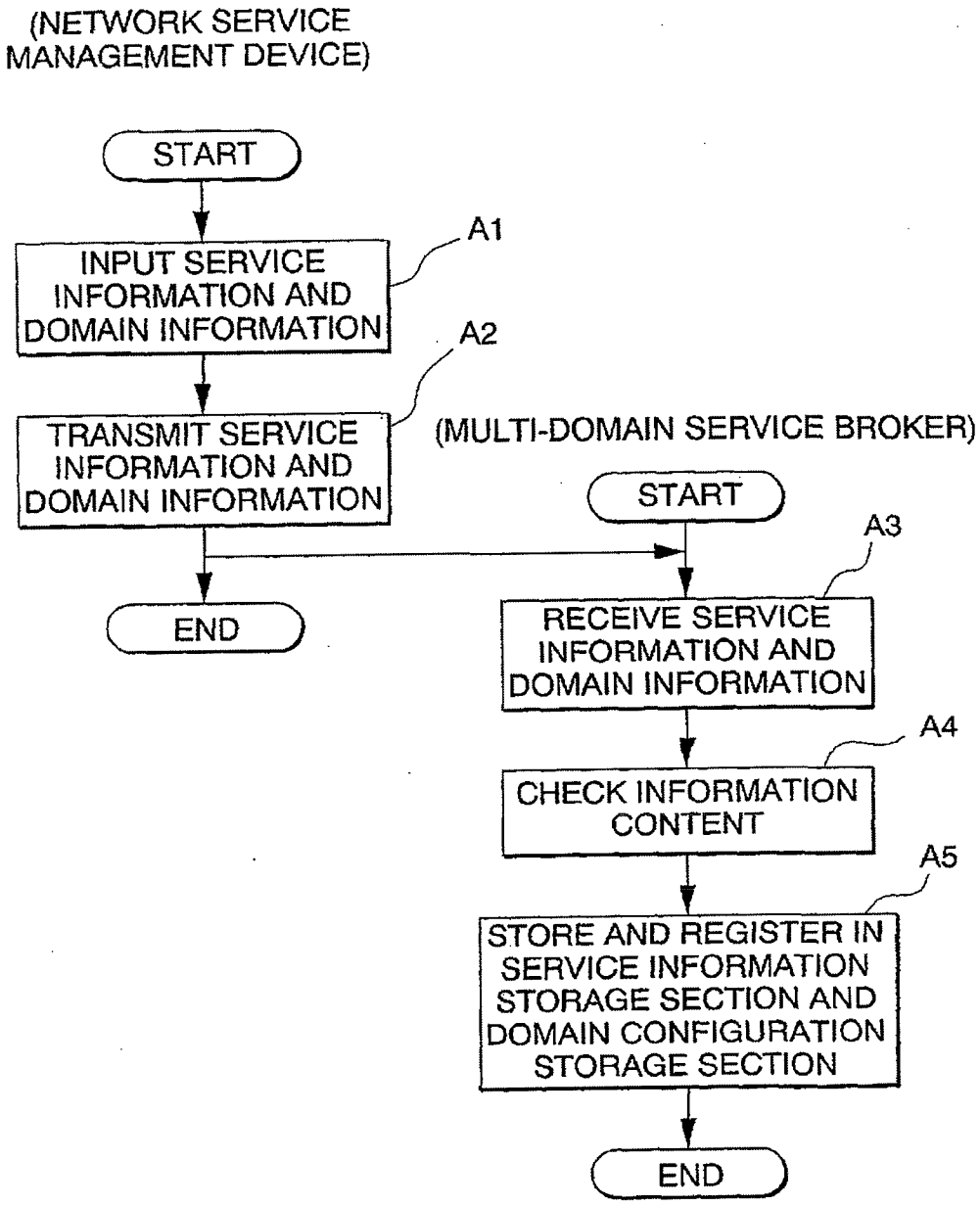

(NETWORK SERVICE MANAGEMENT DEVICE)
START
INPUT SERVICE INFORMATION AND DOMAIN INFORMATION
A1
TRANSMIT SERVICE INFORMATION AND DOMAIN INFORMATION
A2
END
(MULTI-DOMAIN SERVICE BROKER)
START
RECEIVE SERVICE INFORMATION AND DOMAIN INFORMATION
A3
CHECK INFORMATION CONTENT
A4
STORE AND REGISTER IN SERVICE INFORMATION STORAGE SECTION AND DOMAIN CONFIGURATION STORAGE SECTION
A5
END

Fig. 5

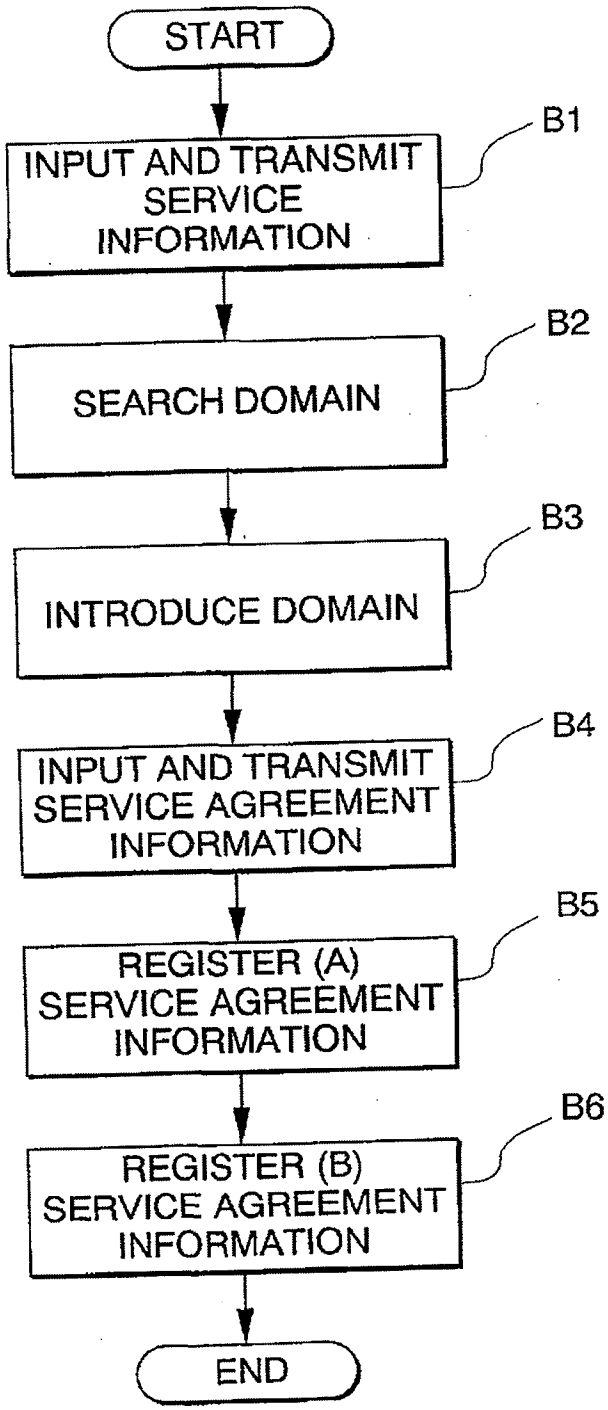

START
INPUT AND TRANSMIT SERVICE INFORMATION
B1
SEARCH DOMAIN
B2
INTRODUCE DOMAIN
B3
INPUT AND TRANSMIT SERVICE AGREEMENT INFORMATION
B4
REGISTER (A) SERVICE AGREEMENT INFORMATION
B5
REGISTER (B) SERVICE AGREEMENT INFORMATION
B6
END

Fig. 6

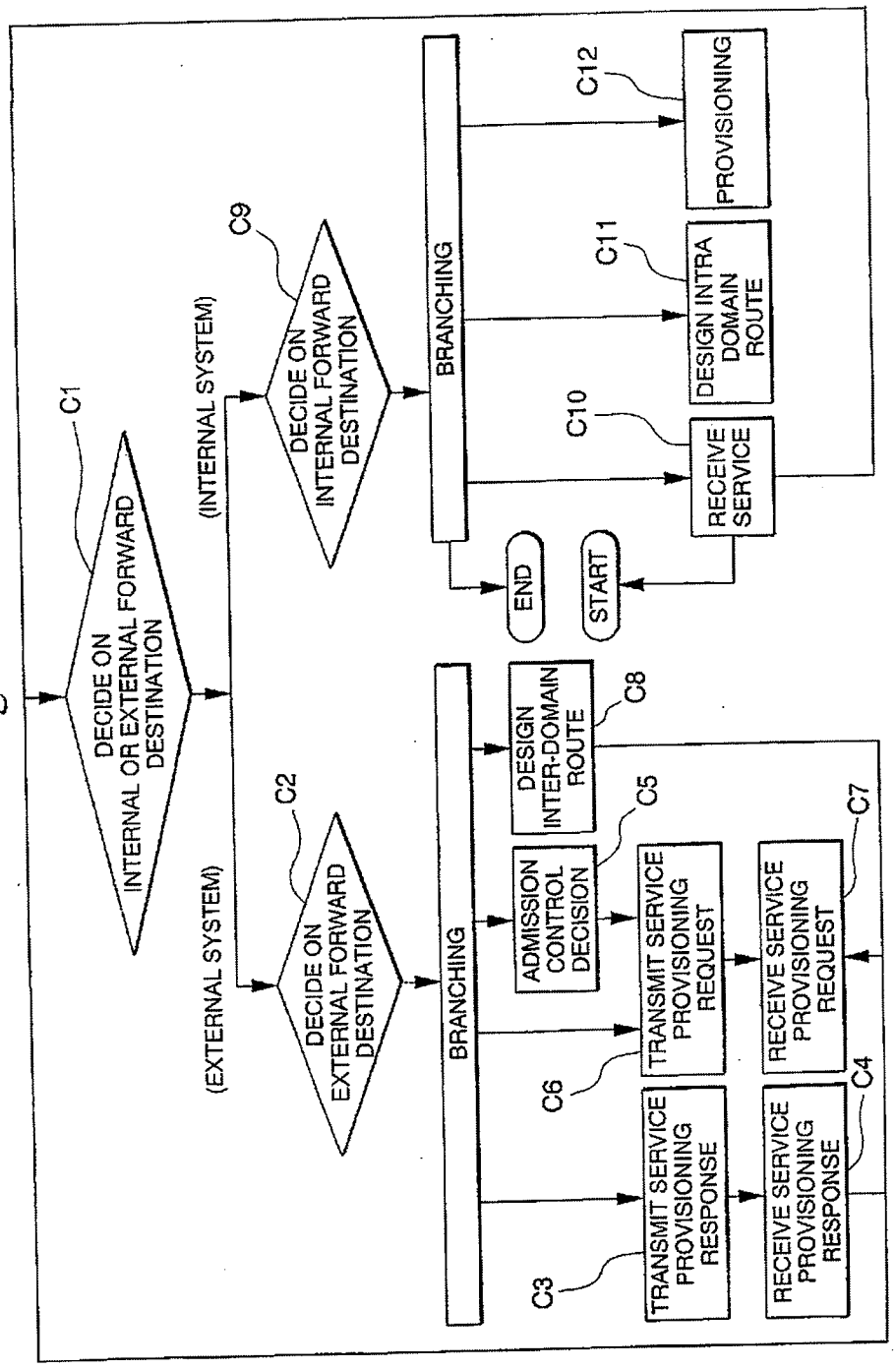

C1
DECIDE ON INTERNAL OR EXTERNAL FORWARD DESTINATION
(INTERNAL SYSTEM)
(EXTERNAL SYSTEM)
C9
DECIDE ON INTERNAL FORWARD DESTINATION
C2
DECIDE ON EXTERNAL FORWARD DESTINATION
BRANCHING
BRANCHING
C12
PROVISIONING
C11
DESIGN INTRA DOMAIN ROUTE
C10
RECEIVE SERVICE
END
START
DESIGN INTER-DOMAIN ROUTE
C8
ADMISSION CONTROL DECISION
C5
TRANSMIT SERVICE PROVISIONING REQUEST
C6
RECEIVE SERVICE PROVISIONING REQUEST
C7
TRANSMIT SERVICE PROVISIONING RESPONSE
C3
RECEIVE SERVICE PROVISIONING RESPONSE
C4

Fig. 7

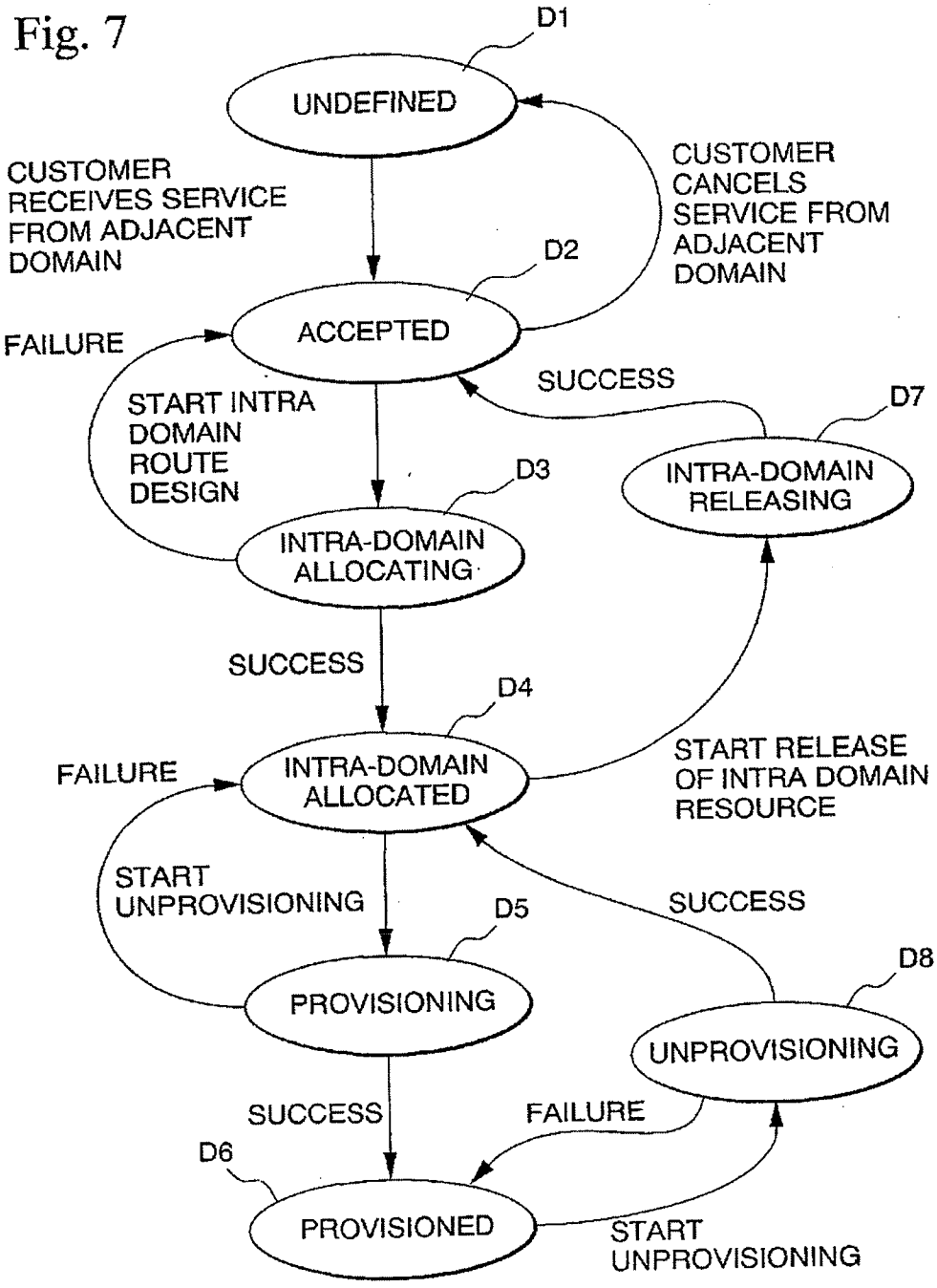
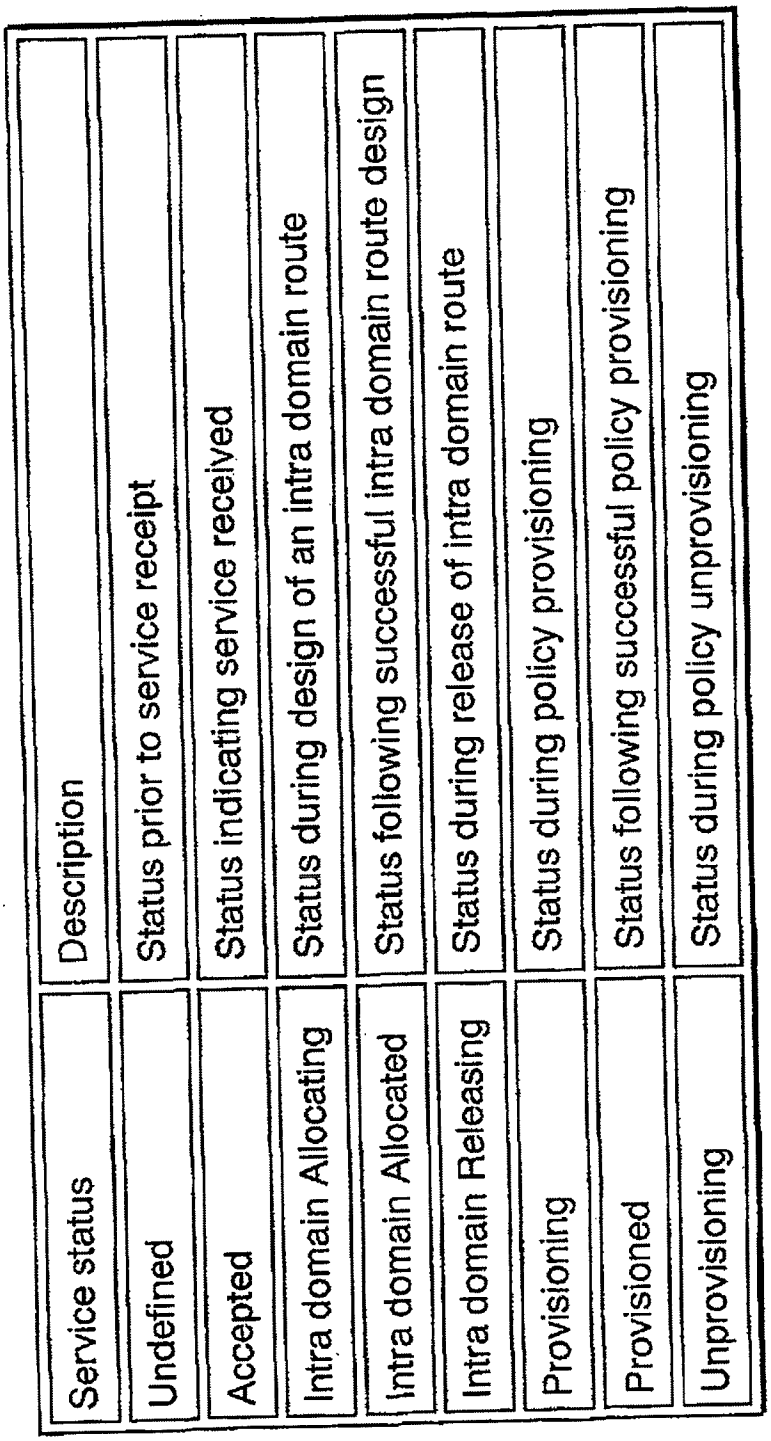

D1
UNDEFINED
CUSTOMER RECEIVES SERVICE FROM ADJACENT DOMAIN
CUSTOMER CANCELS SERVICE FROM ADJACENT DOMAIN
D2
ACCEPTED
FAILURE
SUCCESS
START INTRA DOMAIN ROUTE DESIGN
D7
INTRA-DOMAIN RELEASING
D3
INTRA-DOMAIN ALLOCATING
SUCCESS
D4
FAILURE
INTRA-DOMAIN ALLOCATED
START RELEASE OF INTRA DOMAIN RESOURCE
START UNPROVISIONING
SUCCESS
D5
D8
PROVISIONING
UNPROVISIONING
SUCCESS
FAILURE
D6
PROVISIONED
START UNPROVISIONING

Fig. 8



Service status	Description
Undefined	Status prior to service receipt
Accepted	Status indicating service received
Intra domain Allocating	Status during design of an intra domain route
Intra domain Allocated	Status following successful intra domain route design
Intra domain Releasing	Status during release of intra domain route
Provisioning	Status during policy provisioning
Provisioned	Status following successful policy provisioning
Unprovisioning	Status during policy unprovisioning

Fig. 9

Logic for deciding on either an internal or an external forward destination

(Logic L1) If the current domain is the source domain AND the service status is "Accepted" AND the inter domain route is not designed, transfer to the external system.

(Logic L2) If the current domain is the source domain AND the service status is "Accepted" AND the inter domain route has already been designed, transfer to the internal system.

(Logic L3) If the service status from the source domain to the current domain is "Intra domain Allocated" AND the service status from the downstream domain to the destination domain is "Undefined", transfer to the external system.

(Logic L4) If the current domain is not the source domain AND the service status of the current domain is "Accepted" AND the operation result is " Undefined", transfer to the internal system.

(Logic L5) If the current domain is not the source domain AND the service status of all the domains is "Intra domain Allocated", transfer to the external system.

(Logic L6) If the current domain is the source domain AND the service status of all the domains is "Intra domain Allocated", transfer to the internal system.

(Logic L7) If the service status from the source domain to the current domain is "Provisioned" AND the service status from the downstream domain to the destination domain is "Intra domain Allocated" AND the operation result for the downstream domain is "Undefined", transfer to the external system.

(Logic L8) If the service status from the source domain to the upstream domain is "Provisioned" AND the service status from the current domain to the destination domain is "Intra domain Allocated" AND the operation result for the current domain is "Undefined", transfer to the internal system.

(Logic L9) If there are multiple domains AND the current domain is not the source domain AND the service status of all the domains is "Provisioned", transfer to the external system.

(Logic L10) If there are multiple domains AND the current domain is the source domain AND the service status of all the domains is "Provisioned", transfer to the internal system.

Fig. 10

Logic for deciding an external forward destination

(Logic L11) If the current domain is the source domain AND the service status is "Accepted" AND the inter domain route is not designed, transfer to inter domain route design.

(Logic L12) If the current domain is not the destination domain AND the service status from the source domain to the current domain is "Intra domain Allocated" AND the service status from the downstream domain to the destination domain is "Undefined", transfer to admission control decision.

(Logic L13) If the current domain is not the source domain AND the service status of all the domains is "Intra domain Allocated", transfer to service provisioning request transmission.

(Logic L14) If the current domain is not the destination domain AND the service status from the source domain to the current domain is "Provisioned" AND the service status from the downstream domain to the destination domain is "Intra domain Allocated" AND the operation result for the downstream domain is "Undefined", transfer to service provisioning request transmission.

(Logic L15) If the current domain is not the source domain AND the service status of all the domains is "Provisioned", transfer to service provisioning response transmission.

Fig. 11

Logic for deciding an intra domain forward destination

(Logic L31) If the current domain is the source domain AND the service status is "Accepted" AND the inter domain route is already designed AND the operation result for the current domain is "Undefined", transfer to intra domain route design.

(Logic L32) If the current domain is the source domain AND the service status of all the domains is "Intra domain Allocated", transfer to provisioning.

(Logic L33) If the service status from the source domain to the upstream domain is "Provisioned" AND the service status from the current domain to the destination domain is "Intra domain Allocated" AND the operation result for the current domain is "Undefined", transfer to provisioning.

(Logic L34) If the current domain is the source domain AND the service status of all the domains is "Provisioned", then finish processing.

QUALITY ASSURED NETWORK SERVICE PROVISION SYSTEM COMPATIBLE WITH A MULTI-DOMAIN NETWORK AND SERVICE PROVISION METHOD AND SERVICE BROKER DEVICE

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] The present invention relates to a quality assured network service provision system, a service provision method, and a service broker device for providing a quality assured network service across a plurality of domains managed by different providers.

[0003] 2. Description of the Related Art

[0004] As the Internet has developed, an increasing number of network service providers are providing network services. Against this background, a network service capable of ensuring the end to end quality demanded by customers across a plurality of networks interconnected between different providers has been keenly sought.

[0005] Examples of systems for interconnecting a plurality of this type of communication network are disclosed in the Japanese Unexamined Patent Application, First Publication No. Hei-08-274874 entitled "Network Interconnection Device and Method", and the Published Japanese translation No. 11-501495 of PCT International Publication entitled "Network Link for Interconnecting Service Control Points of Traffic Management Control Load Distribution Groups".

[0006] In a network connection method disclosed in the Japanese Unexamined Patent Application, First Publication No. Hei-08-274874, elements within different electrical communication networks are interconnected, and a mediated access processor (MAP) is provided for connecting an intelligent network for providing service across network boundaries. This MAP enables the conversion, inspection and emulation of messages exchanged between networks, and provides a transparent electrical communication network in which users need not change existing interfaces and protocols.

[0007] Furthermore, in the Published Japanese translation No.11-501495 of PCT International Publication, in order to overcome problems associated with elements of a network becoming overloaded in network environments incorporating a plurality of service providers and multi-vendor devices, an interconnection function is provided by a direct network link between two service control points (SCP) which are used in a load distribution mode.

[0008] This network link involves interconnecting two SCPs within a load distribution group, and as a result offers a method for controlling the SCPs to not only exchange information relating to congestion levels and control functions, but also send queries to an SCP which is not overloaded.

[0009] However, the following problems arise with the conventional technology described above. Namely, in the technique disclosed in the Japanese Unexamined Patent Application, First Publication No. Hei-08-274874, absolutely no consideration is given to operations for provisioning the two interconnected electrical communication networks and providing network services, and so a network service of guaranteed quality cannot be provided via this type of interconnected network.

[0010] Furthermore, the invention disclosed in the Published Japanese translation No. 11-501495 of PCT International Publication simply provides a method for dealing with a network overload, and even in such cases is unable to provide a network service in which the customer is guaranteed sufficient quality.

[0011] In addition, operation information for provisioning the interconnected communication networks and providing network services is not exchanged, and no mechanism is provided for the consistent provision of service form the interconnected network. Moreover, a SCP within a communication device uses a great deal of resources including the CPU, and because a shift to high performance is needed in order to manage the plurality of control function lists, the cost of communication devices deployed within the network increases, and increases in processing loading also become problematic.

[0012] In this manner, conventional networks comprise a plurality of network service providers, and because sufficient consideration has not been given to the provision of uniform quality across the network, there is no option but to provide high performance devices for exchanging information individually within each communication network, and consequently conventional networks have been plagued by problems such as a lack of network expandability and a lack of connection flexibility.

SUMMARY OF THE INVENTION

[0013] The present invention takes the problems inherent in the conventional technology into account, with an object of providing a network service which guarantees the level of quality required by the customer through a plurality of networks operated by different providers, and moreover by incorporating a dedicated service broker device (hereafter referred to as a multi-domain service broker) for managing information which can be provided between providers and designing routes for spanning provider networks, aims to provide a system which is able to achieve function distribution and a high level of expandability.

[0014] A quality assured network service provision system compatible with a multi-domain network according to the present invention is a communication network comprising a plurality of operations management networks (domains) which are connected to a plurality of customer networks with user terminals and which are managed by different providers, which further incorporates a network service management device for managing collectively device clusters incorporated within the operations management network of each provider and receiving service orders and faults information from customers, and a multi-domain service broker at the functional host layer of the network service management device for providing a broker function for enabling agreement between a plurality of providers.

[0015] Moreover, the network service management device comprises information on services which can be provided by each provider, and a device for outputting domain information to the multi-service broker, and the multi-service broker comprises devices for storing output information received

from each network service management device, receiving requests for network service from customers and providing a broker function for achieving agreement between a plurality of providers, selecting the network service management device of a domain which will satisfy the required quality level, and issuing commands for introducing, and then setting, the information necessary for the selected network service management device.

[0016] A first effect of the present invention is the ability to provide a quality assured network service across a plurality of domains managed by different providers. The reason such an effect is achievable is that not only does a design server calculate a communication route within each domain which will satisfy the required level of quality, but that by the exchange of request and response messages between bandwidth brokers, a communication route can be calculated through a plurality of domains. Moreover, the inter domain communication quality is guaranteed by the bandwidth brokers managing the available resource between the domains.

[0017] A second effect is that system maintenance and version upgrades of the customer care server, the policy server, the design server, the network management devices and the workflow server is simple. The reason this effect is achievable is that because only the bandwidth brokers have an interface section with the different providers, it is unlikely that any alterations to the aforementioned servers will have repercussions on the bandwidth brokers.

[0018] A third effect is that the systems of the customer care server, the policy server, the design server, the network management devices and the workflow server can be concealed from other providers. The reason this effect is achievable is that because only the bandwidth brokers have an interface section with the different providers, the only processing visible from an external provider is the interface provided by the bandwidth broker.

[0019] A fourth effect is that an inter domain route from the customer network of the source network to the destination network can be calculated quickly, and furthermore need not be managed by each of the providers. The reason this effect is achievable is that the multi-domain service broker, by managing the service information for all of the associated domains, is able to output the domain cluster which links the source network where the request originated with the destination network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] **FIG. 1** is a structural diagram of a multi-domain network.

[0021] **FIG. 2** is a block diagram showing the functions of a network service management device.

[0022] **FIG. 3** is a block diagram showing the functions of a multi-domain service broker.

[0023] **FIG. 4** is a flowchart showing the sequence within a service registration stage of the present invention.

[0024] **FIG. 5** is a flowchart showing the operations of a service agreement stage of the present invention.

[0025] **FIG. 6** is a flowchart showing the operations of a service provisioning stage of the present invention.

[0026] **FIG. 7** is a transition diagram of service status for the present invention.

[0027] **FIG. 8** is a description of the status labels for the transition diagram of service status.

[0028] **FIG. 9** is a table of logic for deciding on either an internal or an external forward destination.

[0029] **FIG. 10** is a table of logic for deciding an external forward destination.

[0030] **FIG. 11** is a table of logic for deciding an intra domain forward destination.

DETAILED DESCRIPTION OF THE INVENTION

[0031] An object of the present invention is to provide, for a multi-domain network comprising operations management networks (domains) operated by a plurality of network service providers, a network service which guarantees the quality of communication required by a customer in the provision of network services, from end to end, namely from the customer who initiated the request through to the customer at whom the request is directed.

[0032] Then, by introducing a multi-domain service broker for collecting information between the network service management devices provided in each domain, promoting interconnectivity, and brokering the necessary services, a seamless network service provision system can be realized, even between different domains.

[0033] As follows is a description of the construction of an embodiment of the present invention with reference to the drawings. **FIG. 1** is a structural diagram showing a multi-domain network of the embodiment of the present invention, and comprises a plurality of customer networks and a plurality of provider networks. A multi-domain network is a configuration in which customer networks positioned in mutually remote locations are able to communicate with one another via a plurality of provider operations management networks. Specific examples include the case of a network between a head office and a branch office, or the case where affiliated companies create an extranet.

[0034] In the example shown in **FIG. 1**, operations management networks of different providers, namely an operations management network **8** of a provider A and an operations management network **9** of a provider B exist between a customer network E and a customer network D, and each operations management network incorporates a plurality of communication device clusters **3** for performing the processing for the relayed transmission of data.

[0035] In this embodiment, the provision of a service for sending data from the customer network E to the customer network D is taken as an example, and the customer network E is termed the source network **4**, and the customer network D the destination network **5**.

[0036] In order for the communication quality required by the customer to be satisfied from the source network **4** through to the destination network **5**, it is also necessary for both of the intermediate providers A, B to also meet the required communication quality standards of the customer. Here, the term communication quality refers to factors such as delays, fluctuations and bandwidth relating to data traffic.

Consequently, negotiations and cooperative operations are necessary between the provider A and the provider B to agree on communication quality. Furthermore, in order to detect the status of the communication device clusters 3 within each provider, and perform setting and control of specific information, a network service management device 2 is deployed at the functional host layer of the operations management network of each provider A, B.

[0037] (1) Network Service Management Device

[0038] The network service management devices 2 perform management operations such as the management of network configurations, fault management, performance management, security management, customer management and service management, and in particular manage the status of the network within the operations management network and receive service orders and fault reports and the like from customers.

[0039] **FIG. 2** is a block diagram showing the functions of a network service management device. As shown in the diagram, the network service management device incorporates a variety of devices clusters for providing internet connection services, and managing customer information, network information, and provider information. The major components include an input and output device 21 such as a keyboard or a display to enable the operations manager of the provider to input information relating to the services provided by the provider and domain information such as information relating to the operations management network configuration of the provider, a storage device 22 for storing input information on the basis of information type, a workflow server 24 for determining the internal or external forward destination for each processing command, as well as a bandwidth broker 23 for performing registrations of domain information and service information with the multi-domain service broker and cooperating with the workflow server 24 in determining the subject for executing the next process, and internal processing servers such as a customer care server 25 for performing processing within the network service management device, a policy server 26, a design server 27, and a network management device 28.

[0040] As follows is a description of the storage device 22, the bandwidth broker 23, the workflow server 24, and each of the various internal processing servers inside the network service management device 2.

[0041] Storage Device

[0042] The storage device 22 inside the network service management device 2 is a device for storing information on the services provided by the provider and domain information such as information on the configuration of the operations management network offered by the provider, and comprises the following plurality of storage sections for storing each piece of information on the basis of information type; namely, a service level agreement storage section 221, a domain configuration storage section 222, a network configuration storage section 223, a resource storage section 224, a policy storage section 225 and a service storage section 226.

[0043] In this embodiment, a service level agreement storage section 221 is a device for storing agreement information once provider A has reached an agreement with provider B relating to network service, although this issue is described below in further detail. This agreement information includes information relating to communication devices for linking the operations management networks of the provider A and provider B, as well as information on the identification data and type of the circuitry linking the communication devices, information relating to types of service and data traffic profiles, and information on the available hours for the agreement.

[0044] The data traffic profile information incorporates information on bandwidth and communication quality, and for example describes information for providing high priority communication quality in the case where communication data traffic is no more than 10 Mbps, and canceling the communication data when the traffic is greater than 10 Mbps.

[0045] The domain configuration storage section 222 stores domain configuration information for providing network service to customers. Domain configuration information refers to configuration information relating to the operations management network of the provider. For instance, in the example shown in **FIG. 1**, the route from the customer network of the source network through to the customer network of the destination network passes through the operations management network of the provider A and the operations management network of the provider B. In such a case, the link between the operations management network of the provider A and the operations management network of the provider B is stored in the domain configuration storage section 222 as a provider network necessary for providing service.

[0046] The network configuration storage section 223 stores information relating to the communication device clusters 3 inside the operations management network of the provider and the circuitry for linking these communication device clusters 3. The resource storage section 224 stores information relating to the communication devices 3 inside the operations management network of the provider, and includes information such as the total resource capacity, the used resource capacity, and the available resource capacity of each of the communication devices 3. Here, the term resource typically describes the power of the CPU, the memory capacity, and the circuitry bandwidth of the communication device 3. In this embodiment, resources are stored relating to the circuitry bandwidth, although other information could also be stored.

[0047] The policy storage section 225 stores policy which functions as the information for performing settings in the communication devices 3 of the operations management network of the provider. Here, policy refers to the information which should be set in the communication devices 3 for providing network service to a customer, expressed in a manner which is easily understood by an operator, and is described in expressions which are independent of the vendor of the communication device 3. For example in **FIG. 1**, the expression guaranteeing high priority communication data transfer from the customer network E to the customer network D for values of no more than 10 Mbps is one example of this type of policy. The service storage section 226 stores customer information and service information received from customers, such as the service order information describing content guaranteeing high priority communication data transfer from the customer network E to the customer network D for values of no more than 10 Mbps.

[0048] Bandwidth Broker

[0049] Next is a description of the configuration of a bandwidth broker. The bandwidth broker **23** is a system with a data processing function operated by program control, and comprises an external system communication device **233**, a security management device **234**, a service level agreement management device **231**, a domain route management device **232**, and an internal system communication device **235**.

[0050] In this embodiment, the external system communication device **233** is connected to the network service management device cluster **2** of an external system, and to a multi-domain service broker **1**, and provides an interface for communicating with these external systems. The security management device **234** ensures the security of internal systems when communication with an external system is conducted. For example, following connection to an external system, the security management device **234** receives authentication information from the external system, and then only permits information exchange to occur following successful authentication.

[0051] The service level agreement management device **231** registers the service information agreed upon between the providers in the service level agreement storage section **221**, and also manages such information. Furthermore, the service level agreement management device **231** also provides an interface for registering, editing and deleting service level agreement information input via the output device **21**.

[0052] The domain route management device **232** registers the domain linking information necessary for providing network service to customers in the domain configuration storage section **222**, and also manages such information. The internal system communication device **235** provides an interface for the bandwidth broker **23** and the workflow server **24** to communicate.

[0053] Workflow Server

[0054] The workflow server **24**, like the bandwidth broker **23**, is a system with a function for processing data which is operated by program control, and is connected to the bandwidth broker **23**, the customer care server **25**, the design server **27**, the policy server **26**, and the network management device **28** respectively. The workflow server **24** sends the necessary processing commands to each server and manages the progress of the commands in accordance with a workflow and an operation flow defined by the provider.

[0055] Internal Processing Server Cluster

[0056] Next is a description of the remaining customer care server **25**, the policy server **26**, the design server **27** and the network management device **28** which make up the internal processing server cluster for processing and controlling specific settings within the network incorporating the communication devices.

[0057] The customer care server **25** is a system with a data processing function operated by program control, and is connected to the workflow server **24**. The customer care server **25** manages service order information received from customers, and performs the registering of customer information and service information received from customers in the service storage section **226**. Furthermore, the customer care server **25** also provides an interface for the aforementioned service storage section **226** for registering, editing and deleting service information input via the output device **21**.

[0058] The design server **27** is also a system with a data processing function operated by program control, and is connected to the workflow server **24**. The design server **27** manages the internal network resources of the operations management network of the provider, and in the case of this embodiment, manages the total bandwidth, the used bandwidth, and the available bandwidth of the network circuitry.

[0059] When the resource usage status changes, the design server **27** updates the information in the resource storage section **224**, and reads the information from the network configuration storage section **223** in order to refer to the topology information of the operations management network of the provider, thereby always managing the most up to date network resource information. Furthermore, the design server **27** also performs processing for registering policy information as a resource usage plan output in the policy storage section **225**.

[0060] The policy server **26** is a system with a data processing function operated by program control, and is connected to the workflow server **24**. The policy server **26** reads policy information stored in the policy storage section **225**, and converts the policy information into setting information for a communication device **3** specific to a vendor. The policy server **26** then performs provisioning of the communication device **3** in order to enable the provision of service.

[0061] The network management device **28** is a system with a data processing function operated by program control, and is connected to the workflow server **24**. The network management device **28** provides a network fault management function for the configuration and open channel and the like incorporating both the communication devices **3** within the operations management network of the provider, and the connection configuration of the circuitry for connecting these communication devices.

[0062] A network service management device according to the configuration described above provides the necessary information to a multi-domain service broker which provides a broker function for connections between providers, and also provides functions for performing actual settings and control operations on communication devices, based on information supplied from the multi-domain service broker.

[0063] (2) Multi-domain Service Broker

[0064] As follows is a description of the multi-domain service broker **1**. The multi-domain service broker **1** is positioned at the functional host level of the network service management device **2**, and provides a broker function for achieving agreement between a plurality of providers.

[0065] **FIG. 3** is a block diagram showing the functions of the multi-domain service broker **1**. As is shown in **FIG. 3**, the multi-domain service broker **1** comprises an input and output device **11** made up of components such as a keyboard and a display, a data processing device **13** which is operated under program control, and a storage device **12** for storing information.

[0066] The input and output device **11** is connected to a security management device **133**, and is able to perform operations for registering, converting and deleting authentication information and the like used for communications with the network service management device clusters **2** of the providers managed by the multi-domain service broker **1**. The storage device **12** comprises a domain configuration storage section **121** and a service storage section **122**. The domain configuration storage section **121** stores information on the operations management networks of the providers managed by the multi-domain service broker **1** as well as the corresponding connection configurations. In the case of the present embodiment, the operations management networks of the provider A and the provider B are managed by the multi-domain service broker **1**.

[0067] The service storage section **122** stores the services provided by each of the providers. In the case of the present embodiment, this includes network services of high quality, medium quality and low quality for both providers A, B. The data processing device **13** comprises a domain configuration management device **131**, a security management device **133**, a service management device **132** and an external system communication device **134**.

[0068] The domain configuration management device **131** provides operations relating to the provider operations management networks managed by the multi-domain service broker **1**, and provides functions for registering, editing and deleting domain configuration information in the domain configuration storage section **121**. The multi-domain service broker **1** stores domain information which has been registered and declared from the providers in the domain configuration storage section **121**, via the domain configuration management device **131**.

[0069] The security management device **133** performs authentication processing of the network service management devices **2** connected to the multi-domain service broker **1**. Following confirmation of connection with the network service management device **2**, authentication information is received, and if this information is then authenticated by the security management device **133**, data exchange with the network service management device **2** proceeds.

[0070] The service management device **132** manages the services which each provider is able to provide, and also executes the registering, editing and deleting of service information in the service storage section **122**. The external system communication device **134** provides an interface for communication between the multi-domain service broker **1** and the network service management device clusters **2** of each of the providers.

[0071] As follows is a description of the operation of the present invention. In the present invention, cooperation between the network service management device clusters **2** operated by different providers, and the multi-domain service broker **1** enables a customer to be provided with a quality assured network service which spans multiple domains. The keys in this cooperation are the bandwidth broker within each of the network service management device clusters **2**, and the multi-domain service broker **1**.

[0072] The sequence for a quality assured network service provision system compatible with a multi-domain network according to the present invention, can be roughly classified into three main stages, (a) a service registration stage, (b) a service agreement stage, and (c) a service provisioning stage. The operation of the embodiment of the present invention will be described below, with reference to the drawings.

[0073] (a) Service Registration Stage

[0074] The service registration stage is a phase during which the network service management device clusters **2** of each of the providers register with the multi-domain service broker **1**, the domain information and the information on services which can be provided by the operations management network. As a result of the processing of this stage, the multi-domain service broker **1** is able to collect and administer the provider information and the service information for all of the connected operations management networks.

[0075] Specifically, the processing of this service registration stage involves the operations manager for each provider, namely an operator, using the input and output device **11** and inputting information relating to the services provided by the provider, as well as the domain information comprising configuration information on the operations management network of the provider. The information relating to the services provided by the provider and the domain information input in this manner is transmitted to the multi-domain service broker **1** via the external system communication device **233**.

[0076] Furthermore, in this embodiment, the case is described where an operator inputs the service information and domain information for each provider, but the input of this information could also be carried out automatically by pre-programmed conditions, or updated automatically by message information exchanged between customers and each network service management device.

[0077] When the multi-domain service broker **1** receives, via the external system communication device **134**, information relating to the services provided by each provider and the domain information, that received information is stored in the service storage section **122** and the domain configuration storage section **121** respectively of the storage device **12**.

[0078] Next, operation of the service registration stage detailed above will be described with reference to **FIG. 4**. **FIG. 4** is a flowchart showing the sequence within the service registration stage of the present invention.

[0079] First, before the series of operations begins, the network service management device **2** confirms the management information communication connection with the multi-domain service broker **1**, and then following confirmation, the network service management device **2** sends authentication information through the security management device **234**, receives authorization for management information exchange with the multi-domain service broker **1**, and then forms a logical communication path.

[0080] Then, an operations manager or operator uses the input and output device **21** and inputs service information relating to the services the provider A is able to provide, and domain information comprising configuration information for the operations management network of the provider A (step A1). The input service information and domain infor-

mation is transmitted to the multi-domain service broker 1 via the external system communication device 233 (step A2).

[0081] On receipt of the service information and the domain information via the external system communication device 134 (step A3), the multi-domain service broker I first performs a check of the information content (step A4), and if the information is grammatically correct, stores the service information and the domain information in the service storage section 122 and the domain configuration storage section 121 respectively (step A5).

[0082] In this manner, the multi-domain service broker 1 collects domain information and service information from each network service management device of a plurality of providers, and registers this information internally.

[0083] (b) Service Agreement Stage

[0084] Next, in relation to the provision of actual network services to a customer, a service agreement stage is described for reaching agreement on services between operations management networks, in order to enable the provision of network services of equal quality at each of the interconnected providers.

[0085] This service agreement stage corresponds with processing for reaching an agreement on service level by conducting negotiations between the multi-domain service broker 1 and the network service management device clusters, selecting a suitable domain for satisfying the required quality level, and then determining a corresponding communication route, so that when a request is received from a customer, network services of consistent quality can be provided throughout the multi-domain network.

[0086] As follows is a description of the necessity for this agreement on service level. Each provider is able to specify a network quality level based on a variety of parameters such as error rate or delay value, although the level of quality which can be provided, and the method for specifying that level is generally different for different providers. For example, one provider may ask the customer to specify one of three quality levels named Gold, Silver and Bronze, where Gold offers the highest level of quality, whereas another provider may require the customer to specify a quality level based on parameters which may use a different error rate, and may offer a different number of levels (for example, A, B, C, D).

[0087] Consequently, in order to ensure that the quality level requested by the customer is maintained at a constant level within a multi-domain service network, this quality level must be associated with one of the service levels offered within each provider, and a mutual agreement then reached. At this stage, the multi-domain service broker 1 functions as the intermediary broker for reaching service agreements between each of the domains.

[0088] As follows is a brief description of the operation of this service agreement stage. First, an operator at one provider uses the input and output device 21 of the network service management device 2 and inputs service information detailing the conditions desired for a service level agreement. This input service information is transmitted to the multi-domain service broker 1 via the external system communication device 233. On receipt of the service information, the multi-domain service broker 1 uses the service management device 132 to search the service storage section 122, and acquires a domain ID which satisfies the conditions specified.

[0089] Next, the multi-domain service broker 1 uses this domain ID as a key for reading the domain configuration information for that domain from the domain configuration storage section 121, and then transmits this domain information as a response, to the bandwidth broker 23 inside the network service management device cluster 2 where the request originated.

[0090] When the network service management device which receives the response is notified of a certain domain by the multi-domain service broker 1, the operator uses the input and output device 21 and inputs the service level agreement information into the bandwidth broker 23.

[0091] At this point, this service level agreement information transmits a message, via the external system communication device 233 of the network service management device 2, to the bandwidth broker 23 of the adjacent domain introduced by the multi-domain service broker 1, so that the service level agreement information is also registered in the adjacent domain. The processing outlined above is used to reach agreements relating to interconnectivity between the operations management networks of different providers.

[0092] This agreement information includes information on the interconnected communication devices, circuitry, service types, and bandwidths and the like. In this manner, the processing of this service agreement stage involves the exchanging of information and the assigning of service levels relating to the determination of an agreement to enable the provision of network services at the same level of quality across different providers, and results in an agreement relating to service levels between providers.

[0093] Next is a description of the specifics of the service agreement stage with reference to FIG. 5. The service agreement is made between different providers, and is a convention relating to the interconnectivity between operations management networks.

[0094] An operator at the provider A (hereafter referred to as the operator A) uses the input and output device 21 and inputs service information detailing the conditions desired for a service level agreement. This service information includes information such as service classifications for high priority, medium priority and low priority service. This input service information is transmitted to the multi-domain service broker 1 via the external system communication device 233 (step B1).

[0095] When the multi-domain service broker 1 receives this service information, the service management device 132 searches the service storage section 122, and acquires a domain ID which satisfies the conditions specified (step B2).

[0096] Then, the domain configuration management device 131 uses this domain ID as a key and acquires the domain information from the domain configuration storage section 121. The multi-domain service broker 1 then transmits a response to the bandwidth broker 23 of the provider A (hereafter referred to as the bandwidth broker A) via the external system communication device 134. On receipt of this domain information, the bandwidth broker 23 inputs the

domain information into the input and output device **21**. In the case of this embodiment, the domain of the provider B (hereafter referred to as the domain B) is introduced (step B3).

[0097] The operator A specifies the domain B and inputs the service level agreement information. The service level agreement information includes information on service classes such as high priority, medium priority and low priority service, as well as information on required communication quality. In this embodiment, bandwidth information is input. The service level agreement information is transmitted to the bandwidth broker **23** of the provider B (hereafter referred to as the bandwidth broker B) via the external system communication device **233** (step B4).

[0098] Before the transmissions from the above series of processing are conducted, the bandwidth broker A confirms the management information exchange connection with the bandwidth broker B, and receives authentication. This authentication is performed by the security management device **234**.

[0099] On receipt of the service level agreement information, the bandwidth broker B checks the content of the data. If there are no grammatical errors, then the service level agreement management section **231** inside the bandwidth broker B (hereafter referred to as the service level agreement management section B) acquires information from the service level agreement storage section **221** on the available resource capacity between the domain A and the domain B, and service information relating to high priority, medium priority and low priority service levels. If an agreement is possible, then a response is transmitted to the bandwidth broker A via the external system communication section B, and the service agreement information agreed upon with the provider A is registered in the service level agreement storage section B (step B5).

[0100] The bandwidth broker A receives the response, and if the service level agreement request has been accepted, registers that agreement information in the service level agreement storage section A (step B6).

[0101] The processing outlined above is used to reach agreement relating to interconnectivity between the operations management networks of the provider A and the provider B. This agreement information includes information on the interconnected communication devices, circuitry, service types, and bandwidths and the like.

[0102] (c) Service Provisioning Stage

[0103] Next, the service provisioning stage is executed. Service provisioning is a step where, based on a service order from a customer, operations are performed for setting and controlling information in the communication devices so that a service can be operated between customer networks via the operations management networks of a plurality of providers.

[0104] This service provisioning stage can be further classified into three stages, namely, service order processing, route design processing, and provisioning processing. These three stages of processing are executed mainly by a customer care server, a design server, and a policy server respectively.

[0105] The workflow server **24** controls this cluster of servers in accordance with the operation flows for the provision of network services, and the workflow server **24** also controls the cooperative operation of the customer care server **25**, the design server **27**, the policy server **26** and the workflow server **24** and the like inside the network service management device of each domain.

[0106] In other words, service order processing refers to the processing in the customer care server **25** for receiving and processing service order information received from a customer, and registering that information in the service storage section **226**, and route design processing refers to the processing in the design server **27**, which manages the internal network resources of the operations management network of the provider, for managing the total bandwidth, the used bandwidth, and the available bandwidth of the network circuitry, and determining an actual route depending on the usage status of the resources. Moreover, the provisioning processing refers to the processing for reading the policy information stored in the policy storage section **225** by using the policy server **26**, and converting this information to setting information for a communication device of a specific vendor. Provisioning for providing service refers to control processing performed on a communication device **3**.

[0107] As follows is a description of processing examples of the service order processing, the route design processing and the provisioning processing from the service provisioning stage.

[0108] First, in the case of service order processing, a customer requests a service order from the provider A, and the operator A uses the input and output device **21** of the network service management device **2** to register this service order information in the customer care server **25**. The customer care server **25** then stores the information input by the operator A in the service storage section **226**.

[0109] Next, in the route design processing, processing is performed for designing an inter domain connection route between domains, and for designing an intra domain route within the domain. Of these two, the former is equivalent to the processing for calculating linkages for the operations management networks of the providers positioned between the customer network of the source network through to the destination network, and is carried out by the multi-domain service broker **1**. The latter is equivalent to processing for calculating linkages between communication devices **3** within the operations management network of the provider, and is carried out by the design server **27**.

[0110] First, in order to design an inter domain connection route, the bandwidth broker **23** of the network service management device **2** transmits a request message to the multi-domain service broker **1** via the external system communication device **233**.

[0111] The multi-domain service broker **1** executes the inter domain route design process, and a response is then transmitted from the multi-domain service broker **1** back to the bandwidth broker **23**.

[0112] Subsequently, the design server **27** designs an intra domain route which will satisfy the level of communication quality requested. The results of this intra domain route

design process executed by the design server **27** are written to the resource storage section **224** and the policy storage section **225**.

[0113] In the resource storage section **224**, the resource information is updated with the newly allocated network resource information produced as a result of the route design process. In the policy storage section **225**, the configuration data for setting the communication devices within the network is written as policy.

[0114] Next, the service level agreement management device **231** of the bandwidth broker **23** refers to the service level agreement storage section **221**, and checks whether or not the service information requested by the customer can be accommodated by a service agreed upon between the provider A and the provider B.

[0115] In those cases where the service can be accommodated, the network service management device **2** transmits a provisioning request message to the bandwidth broker **23**A of the adjacent domain, via the external system communication device **233**.

[0116] When the bandwidth broker **23**B of the adjacent domain receives the provisioning request, the design server **27** of the network service management device of that adjacent domain calculates an intra domain route which will satisfy the level of communication quality requested.

[0117] Then, as a result of this calculation process, the bandwidth broker **23**B of this adjacent domain transmits a service provisioning response to the bandwidth broker where the request originated. In this manner, the registration of service orders, and the intra domain and inter domain design processes are executed by the service order processing stage and the route design processing stage.

[0118] In the third stage of provisioning processing, the actual setting and control of the configuration information in the appropriate communication devices is conducted, based on the route information and the like designed in the manner descried above. In other words, the policy server **26** reads the configuration data required for the communication devices **3** to provide the service, from the policy storage section **225**. Here, the object of the provisioning performed by the policy server **26** is the operations management network of the provider.

[0119] Next the bandwidth broker **23**A acquires the linkage information for those domains which are passed through in order to provide the service, and then transmits a service provisioning request message to the bandwidth broker **23**B of the adjacent domain.

[0120] When the bandwidth broker **23**B of the adjacent domain receives the service provisioning request message, the policy server **26** reads the policy data for that particular service from the policy storage section **225**. Then, provisioning is executed for the communication devices **3** within the operations management network of the domain which relate to that service.

[0121] The bandwidth broker **23** of the adjacent domain then transmits a service provisioning response message to the bandwidth broker **23** where the request originated.

[0122] On receipt of this service provisioning response message from the adjacent domain, the bandwidth broker **23** finishes processing, and a communication service which passes through a plurality of domains is provided.

[0123] As follows is a detailed description of the service provisioning stage with reference to **FIG. 6** and **FIG. 7**. **FIG. 6** is flowchart showing the operations of the service provisioning stage of the present invention. **FIG. 7** is a transition diagram of service status relating to the present invention.

[0124] In the flowchart of **FIG. 6** there are a plurality of execution blocks. The block labeled "decide on internal or external forward destination" (step C1) shown at the top of the diagram refers to processing performed by the bandwidth broker **23** or the workflow server **24**.

[0125] Furthermore, the blocks labeled "decide on external forward destination" (step C2), "admission control decision" (step CS), "transmit service provisioning response" (step C3), "receive service provisioning response" (step C4), "transmit service provisioning request" (step C6), and "receive service provisioning request" (step C7), shown down the left hand side of the diagram refer to processing performed by the bandwidth broker **23**.

[0126] The block labeled "design inter domain route" (step C8) is performed by the multi-domain service broker **1**. The block labeled "decide on internal forward destination" (step C9) shown on the right of the diagram is performed by the workflow server **24**. The block labeled "receive service" (step C10) is executed by the customer care server **25**, whereas the blocks labeled "design intra domain route" (step C11) and "provisioning" (step C12) are executed by the design server **27** and the policy server **26** respectively.

[0127] Moreover, at the provisioning stage, the status of the services provided to customers in each of the domains is managed. **FIG. 7** shows a transition diagram for service status.

[0128] First, a customer places a service order request with the provider A. The service order includes information on the location of the customer network and information on the communication quality. In this embodiment, service classes such as high priority and the like and required bandwidth values are declared for the customer network E and the customer network D.

[0129] In the following description, the situation is described where the multi-domain service broker **1** selects the provider B as the provider which can provide the desired communication service for the received service order at the provider A. Furthermore, in the description, the functional devices and blocks which correspond with those shown in the configurations of **FIG. 2** and **FIG. 3** are labeled with the same numerals, although the letters A and B are added to indicate the appropriate provider.

[0130] In the provider A, the received service order information is registered in the customer care server **25**A by the operator A, using the input and output device **21** A. The customer care server **25**A performs a grammatical check of the data, and if the data is grammatically correct, stores the data in the service storage section **226**A (step C10 of **FIG. 6**). Furthermore, the service status is stored as "Accepted" (state D1 of **FIG. 7**).

[0131] Next, a decision is made by the workflow server **24A** to specify either an internal or an external forward destination (step C1).

[0132] As shown in **FIG. 9**, this decision on an internal or external forward destination is executed by referring to the service status stored in the service storage section **226A**, using logic incorporated in the sever or the system as the program control. **FIG. 9** is a logic diagram for deciding on either an internal or an external forward destination. **FIG. 10** is a logic diagram for deciding an external forward destination, and **FIG. 11** is a logic diagram for deciding an intra domain forward destination.

[0133] The logic for deciding a forward destination uses the service status, operation results, and the location of linkage between each of the providers interconnected in order to provide the service. The status of the service received from the customer is managed according to the service status transition diagram shown in **FIG. 7**, and the status of intra domain route design and service provisioning can be obtained in terms such as non-executed, successful or failed. These states are managed by the respective servers, although a configuration is also possible where a device is provided within a separate network service management device for collectively managing the aforementioned service status for each device cluster, with each of the servers then writing to, or referring to this device as necessary. Because the trigger for causing a transition in status is the execution of an operation in a device such as the customer care server, the design server or the policy server shown in **FIG. 2**, by referring to the service status, the server requiring processing can be determined.

[0134] Furthermore, location within the domain linkage is classified into three sections, namely the source domain, a middle domain, and the destination domain. The source domain refers to the provider network connected with the source network of the customer. The destination domain refers to the provider network connected with the destination network of the customer. The middle domain refers to a provider network located between the source domain and the destination domain which provides network resources to the customer. For example, in the case where three providers A, B, C exist, and the provider A accommodates the source network of the customer and the provider C accommodates the destination network of the customer, then the provider B is the middle domain. This information is identified and managed within the network service management device.

[0135] Furthermore, there are three possible operation results, namely "Undefined", "OK" and "NG". The result "Undefined" describes non-execution of the operation, "OK" describes a successful operation, and "NG" describes an operation failure.

[0136] In the logic for deciding on either an internal or an external forward destination according to the workflow server **24A**, in the case where the current domain is the source domain AND the service status is "Accepted" AND the inter-domain route has not been designed, processing is transferred to the external system (logic L1). Here, an external system refers to an external device outside of the internal processing server cluster of the network service management device, and so processing transfers from the workflow server **24A** of the provider A to the bandwidth broker **23A**.

[0137] Then, the bandwidth broker **23A** receives the processing and makes a decision on an external forward destination (step C2). At this point, the current domain is the source domain AND the service status is "Accepted" AND the inter-domain route has not been designed, and so the processing transfers to inter-domain route design (logic L11). In other words, a processing transfer request message is transmitted to the multi-domain service broker **1** via the external system communication device **233A**.

[0138] Next, the multi-domain service broker **1** executes the inter-domain route design process (step C8). In the inter-domain route design process, the domain configuration management device **131** and the service management device **132** refer to the domain configuration storage section **121** and the service storage section **122** respectively and design a domain linkage which will satisfy the service requested by the customer.

[0139] Here the domain linkage refers to the provider network linking the source network of the customer network with the destination network. Following completion of the inter-domain route design, a response is transmitted from the multi-domain service broker **1** to the bandwidth broker **23A** of the provider A.

[0140] The bandwidth broker **23A** of the provider A then receives the aforementioned processing and makes a decision on either an internal or an external forward destination (step C1). At this time, the current domain is the source domain AND the service status is "Accepted" AND the inter-domain route has already been designed, and so the processing transfers to the internal system (logic L2). In other words, processing transfers to the workflow server **24A** of the provider A.

[0141] Subsequently, the workflow server **24A** makes a decision on an internal forward destination (step C9). At this point, the current domain is the source domain AND the service status is "Accepted" AND the inter-domain route has already been designed AND the operation result from the current domain is "Undefined", and so the processing transfers to intra domain route design (logic L31). In other words, the design server **27** designs an intra domain route which will satisfy the required communication quality (step C11).

[0142] The result of the intra domain route design process executed by the design server **27** is written into the resource storage section **224** and the policy storage section **225**. In the resource storage section **224**, the resource information is updated with the newly allocated network resource information from the design process. For example, if in a bandwidth of 10 Mbps, 1.5 Mbps is used and a further 1.5 Mbps is newly allocated, then this amounts to 3.0 Mbps of resource being allocated. In the policy storage section **225**, the configuration data for setting the communication devices **3** within the network is written as policy.

[0143] Next, the workflow server **24A** of the provider A makes a decision on either an internal or an external forward destination (step C1). At this point, the service status from the source domain to the current domain is "Intra domain Allocated" AND the service status from a downstream domain to the destination domain is "Undefined", and so the processing transfers to the external system (logic L3). In other words, the processing transfers to the bandwidth broker **23A**.

[0144] Subsequently, the bandwidth broker 23A decides on an external forward destination (step C2). At this point, the current domain is not the destination domain AND the service status from the source domain to the current domain is "Intra domain Allocated" AND the service status from the downstream domain to the destination domain is "Undefined", and so the processing transfers to the admission control decision process (logic L22, step C5).

[0145] In the case of this embodiment, the linkage between the operations management network of the provider A and the operations management network of the provider B is determined around service to the customer, and so the service level agreement management device 231 A of the provider A refers to the service level agreement storage section 221A and checks whether or not the service information requested by the customer can be accommodated by the services agreed upon between the provider A and the provider B. In those cases where such accommodation is impossible, an error message is displayed on the input and output device 21A and the processing ends. In those cases where the service can be accommodated, a service provisioning request is transmitted to the bandwidth broker 23B of the provider B (the bandwidth broker B) via the external system communication device 233A (step C6).

[0146] On receipt of the service provisioning request (step C7), the bandwidth broker 23B executes the logic for deciding on either an internal or an external forward destination (step C 1). At this point, the current domain is not the source domain AND the service status of the current domain is "Accepted" AND the operation result is "Undefined", and so the processing transfers to the internal system (logic L4). In other words, the processing transfers to the workflow server 24B.

[0147] The workflow server 24B then executes the logic for deciding on an internal forward destination (step C9). At this point, the current domain is the source domain AND the service status is "Accepted" AND an inter-domain route has already been designed AND the operation result from the current domain is "Undefined", and so processing transfers to intra domain route design (logic L31).

[0148] Next, the design server 27B designs an intra domain route which will satisfy the required communication quality (step C11), and then transfers processing to the workflow server 24B.

[0149] The workflow server 24B then executes the logic for deciding on either an internal or an external forward destination (step C1).

[0150] At this point, the current domain is not the source domain AND the service status for all domains is "Intra domain Allocated", and so processing transfers to the external system (logic L5). In other words, the processing transfers to the bandwidth broker 23B.

[0151] Subsequently, the bandwidth broker 23B executes the logic for deciding an external forward destination (step C2). The domain route management device 232B inside the bandwidth broker 23B acquires, from the domain configuration storage section 222B, the domain linkage information needed to achieve the service to be provided to the customer. In the case of this embodiment, the linkage between the operations management network of the provider A and the operations management network of the provider B is registered, and so a service provisioning response is transmitted to the network service management device cluster 2A, namely to the bandwidth broker 23A (step C3).

[0152] On receipt of the service provisioning response from the bandwidth broker 23B via the external system communication device (step C4), the bandwidth broker 23A executes the logic for deciding on either an internal or an external forward destination (step C1).

[0153] In the case of this embodiment, at this point the current domain is the source domain AND the service status for all domains is "Intra domain Allocated", and so processing transfers to the internal system (logic L6). In other words, processing transfers to the workflow server 24A via the internal system communication device of the bandwidth broker 23A.

[0154] Next, the workflow server 24A decides on an internal forward destination within the network service management device cluster 2A (step C9). At this point, the current domain is the source domain AND the service status for all domains is "Intra domain Allocated", and so the next process is provisioning (logic L32). In other words, processing transfers to the policy server 26A. At this time, the objective service ID is passed from the workflow server 24A to the policy server 26A.

[0155] The policy server 26A uses the service ID as a key and reads the configuration data for the communication devices required for providing the desired service from the policy storage section 225A. In the case of this embodiment, the policy server 26A conducts provisioning on the operations management network of the provider A.

[0156] Next, the policy server 26A converts the read policy data to configuration data specific to the communication device, and executes provisioning (step C12). Typically, setting commands and data for the communication device 3 will vary depending on the maker of the communication device, but policy data is configuration data which is independent of each communication device.

[0157] Consequently, the policy server converts the policy data into setting commands and data which correspond with each of the communication devices, and then executes provisioning. If provisioning succeeds, then the service status of the current domain is changed from "Intra domain Allocated" to "Provisioned", and then stored in the service storage section 226. Furthermore, the operation result for the current domain provisioning is subsequently treated as "OK".

[0158] Once the policy server 26A has executed provisioning, the processing transfers to the workflow server 24A, and a decision is made on either an internal or an external forward destination (step C1). In the case of this embodiment, at this point the service status from the source domain to the current domain is "Provisioned" AND the service status from the downstream domain to the destination domain is "Intra domain Allocated", AND the operation result for the downstream domain is "Undefined", and so the processing transfers to the external system (logic L7). In other words, the processing transfers from the workflow server 24A to the bandwidth broker 23A.

[0159] Next, the bandwidth broker 23A executes the logic for deciding an external forward destination (step C2). In

this embodiment, at this point the current domain is not the source domain AND the service status for all the domains is "Intra domain Allocated", and so the next process is the service provisioning request transmission process (logic L23).

[0160] The bandwidth broker 23A acquires, from the domain configuration storage section 222A, the linkage information for those domains which are passed through in order to provide the service. In the case of this embodiment, the linkage is between the operations management network of the provider A and the operations management network of the provider B, and so the bandwidth broker 23A transmits a service provisioning request message for transferring the processing to the bandwidth broker 23B (step C6).

[0161] On receipt of the service provisioning request message (step C7), the bandwidth broker 23B checks whether or not the message is grammatically correct.

[0162] If the message is grammatically correct, then the bandwidth broker 23B executes the logic for deciding on either an internal or an external forward destination (step C1). At this point, in this embodiment, the service status from the source domain to the upstream domain is "Provisioned" AND the service status from the current domain to the destination domain is "Intra domain Allocated", AND the provisioning operation result for the current domain is "Undefined", and so the processing transfers to the internal system (logic L8). In other words, the processing transfers to the workflow server 24B via the internal system communication device 235.

[0163] The workflow server 24B then executes the logic for deciding on an internal forward destination within the network service management device cluster B (step C9).

[0164] In the case of this embodiment, at this point the service status from the source domain to the upstream domain is "Provisioned" AND the service status from the current domain to the destination domain is "Intra domain Allocated", AND the operation result for the current domain is "Undefined", and so the next process is provisioning (logic L33). In other words, processing transfers to the policy server 26B. At this time, the service ID which is the object of the provisioning process passes to the policy server 26B.

[0165] The policy server 26B uses the service ID as a key and reads the policy data for the service from the policy storage section 225B. The policy server 26B then executes provisioning on those communication devices 3 within the operations management network of the provider B which relate to the service, and then updates the service status based on the results of the provisioning. If the provisioning succeeds, then the service status is changed to "Provisioned" and the processing transfers to the workflow server 24B.

[0166] The workflow server 24B of the provider B then executes the logic for deciding on either an internal or an external forward destination (step C1). In the case of this embodiment, there are multiple domains AND the current domain is not the source domain AND the service status of all the domains is "Provisioned", and so the processing transfers to the external system (logic L9). In other words, the processing transfers from the workflow server 24B to the bandwidth broker 23B.

[0167] On receipt of the message from the workflow server 24B, the bandwidth broker 23B executes the logic for deciding an external forward destination (step C2). In this embodiment, at this point the current domain is not the source domain AND the service status for all the domains is "Provisioned", and so the next process is the service provisioning response transmission process (logic L25).

[0168] The bandwidth broker 23B acquires the domain linkage information needed to achieve the service from the domain configuration storage section 222B. In this embodiment the upstream domain from the operations management network of the provider B is the provider A, and so the bandwidth broker 23B transmits a service provisioning response message to the bandwidth broker 23A via the external system communication device 233 (step C3).

[0169] On receipt of the service provisioning response message from the bandwidth broker 23B (step C4), the bandwidth broker 23A executes the logic for deciding on either an internal or an external forward destination (step C1). In the case of this embodiment, there are multiple domains AND the current domain is the source domain AND the service status of all the domains is "Provisioned", and so the processing transfers to the internal system (logic L10). In other words, the processing transfers from the bandwidth broker 23A to the workflow server 24A.

[0170] Next, the workflow server 24A executes the logic for deciding on an intra domain forward destination (step C9). In the case of this embodiment, at this point the current domain is the source domain AND the service status of all the domains is "Provisioned", and so the processing finishes (logic L34).

[0171] As described above, by making the network service management device cluster 2A of the provider A and the network service management device cluster 2B of the provider B cooperate in the execution of a service registration stage, a service agreement stage and a service provisioning stage, network service can be provided via a plurality of domains.

What is claimed is:

1. A quality assured network service provision system compatible with a multi-domain network, wherein

a communication network comprising a plurality of operations management networks (domains) which are connected to a plurality of customer networks with user terminals and which are managed by different providers, includes:

a network service management device for managing collectively device clusters incorporated within an operations management network of each of said providers, and receiving service orders and faults information from customers; and

a service broker device at the functional host layer of said network service management device cluster for providing a broker function for achieving agreement between said plurality of providers.

2. A quality assured network service provision system compatible with a multi-domain network according to claim 1, wherein

said network service management device comprises an outputting device for outputting information on ser-

vices which can be provided by each of said providers and domain information to said multi-service broker; and

said service broker device comprises a device for storing output information from each network service management device, selecting a network service management device of a domain which will satisfy a required quality level when a network service request is generated by a customer, and issuing instructions for introducing and setting necessary information.

3. A quality assured network service provision system compatible with a multi-domain network according to claim 2, wherein

said network service management device comprises an input and output device for input, by an operator, of information on services which can be provided by said provider and domain information made up of configuration information about an operations management network of said provider;

storage devices for storing information input from said input and output device by information type;

a workflow server for determining transfer destinations for processing commands based on each service request from a customer;

a bandwidth broker for registering said domain information and service information in said service broker device, and determining, in cooperation with said workflow server, a subject for executing a subsequent process; and

an internal processing system for performing processing management of information required by said communication device.

4. A quality assured network service provision system compatible with a multi-domain network according to claim 2, wherein

said service broker device comprises a storage device for storing service information and domain information received from said network service management device; and

a data processing device for performing information processing such as writing and reading of information to and from said storage device, as well as providing a security management function relative to said bandwidth broker.

5. A quality assured network service provision system compatible with a multi-domain network according to claim 3, wherein

said bandwidth broker and said workflow server have a means for deciding, based on logic, whether a subject for executing a subsequent process due to a customer service request is in an external system or an internal system; and

said bandwidth broker has a means for deciding a domain in cases where a subject for executing a subsequent process is in an external system; and

said workflow server has a means for deciding an internal processing system of a forward destination in cases where a subject for executing a subsequent process is in an internal system.

6. A quality assured network service provision system compatible with a multi-domain network according to claim 3, wherein

said service broker device has a means for referring to service information stored in said service storage section and deciding whether a subject for executing a subsequent process due to a customer service request is in an external system or an internal system;

a means for deciding an external forward destination in cases where a subject for executing a subsequent process is in an external system; and

a means for deciding an internal processing system of a forward destination in cases where a subject for executing a subsequent process is in an internal system.

7. A quality assured network service provision system compatible with a multi-domain network according to claim 3, wherein

said internal system comprises any one of a customer care server for managing service order information received from customers,

a design server for managing network resources of an operations management network of a provider,

a policy server for reading pre-recorded policy information, as well as converting said policy information into setting information for a communication device of a specific vendor, and performing provisioning of a communication device for the provision of a service, and

a network management device for providing a network fault management function for a configuration management and open channel incorporating communication devices within an operations management network of a provider and connection configuration of circuitry for connecting said communication devices, each of which is connected to said workflow server.

8. A method of providing a quality assured network service compatible with a multi-domain network comprising

a plurality of domains which are connected to a plurality of customer networks with user terminals and which are managed by different providers, and incorporating

a network service management device for controlling collectively device clusters incorporated within an operations management network of each of said providers, as well as receiving service orders and faults information from customers, and

a service broker device at the functional host layer of said network service management device cluster for providing a broker function for achieving agreement between said plurality of providers, wherein said method comprises:

a service registration step in which a network management device of each provider registers in said service broker device, domain information comprising configuration information and information on services which can be provided,

a service agreement step in which a request is received from a customer, said service broker device and said network management device reach an agreement relating to service conditions for providing a service which will satisfy a required quality level, and route information for an appropriate domain and a network management device are selected, and

a service provisioning step for performing required service provisioning on a communication device based on service conditions and route information agreed upon in said network management device.

9. A method of providing a quality assured network service compatible with a multi-domain network according to claim 8, wherein said service provisioning step further comprises a step for service order processing, a step for route design processing, and a step for provisioning processing.

10. A service broker device in an interconnected network for providing, in a network comprising a plurality of operations management networks which are connected to a plurality of customer networks with user terminals and which are managed by different providers,

a broker function for achieving agreement between a plurality of providers based on configuration information and information on the services which can be provided by each provider network.

* * * * *

(Document 2)

(12) PATENT APPLICATION **(11)** Application No. **AU 199944769 A1**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
A system for managing a telecommunications network

(51)[6] International Patent Classification(s)
G06F 017/60 **H04L 012/02**

(21) Application No: **199944769** (22) Application Date: **1999.08.26**

(30) Priority Data

(31) Number	(32) Date	(33) Country
98 10759	**1998.08.27**	**FR**

(43) Publication Date : **2000.03.09**
(43) Publication Journal Date : **2000.03.09**

(71) Applicant(s)
Alcatel

(72) Inventor(s)
Laurent Carre

(74) Agent/Attorney
FREEHILLS PATENT ATTORNEYS,Level 32, MLC Centre,Martin Place,SYDNEY NSW 2000

A B S T R A C T

The invention relates to a system for managing telecommunications networks, the system having one or more network information management modules (IM1/IM2), and one or more user service modules (USM). According to the invention, the management system is fitted with software architecture including an interface (f) suitable for supporting one or more user presentation layers (CP) for a user services management module (USM).

FIG_1

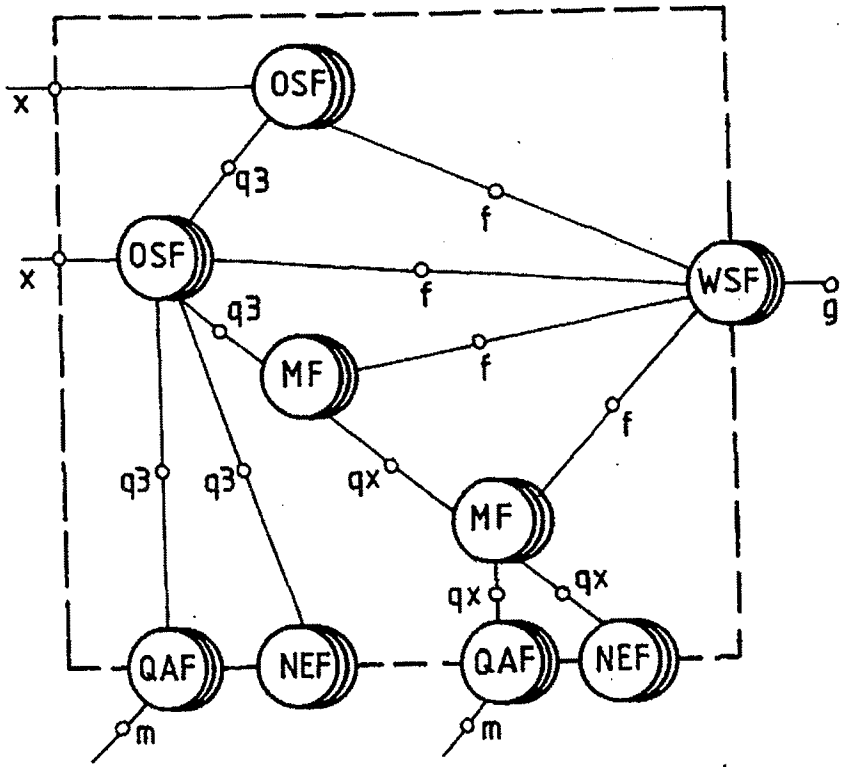
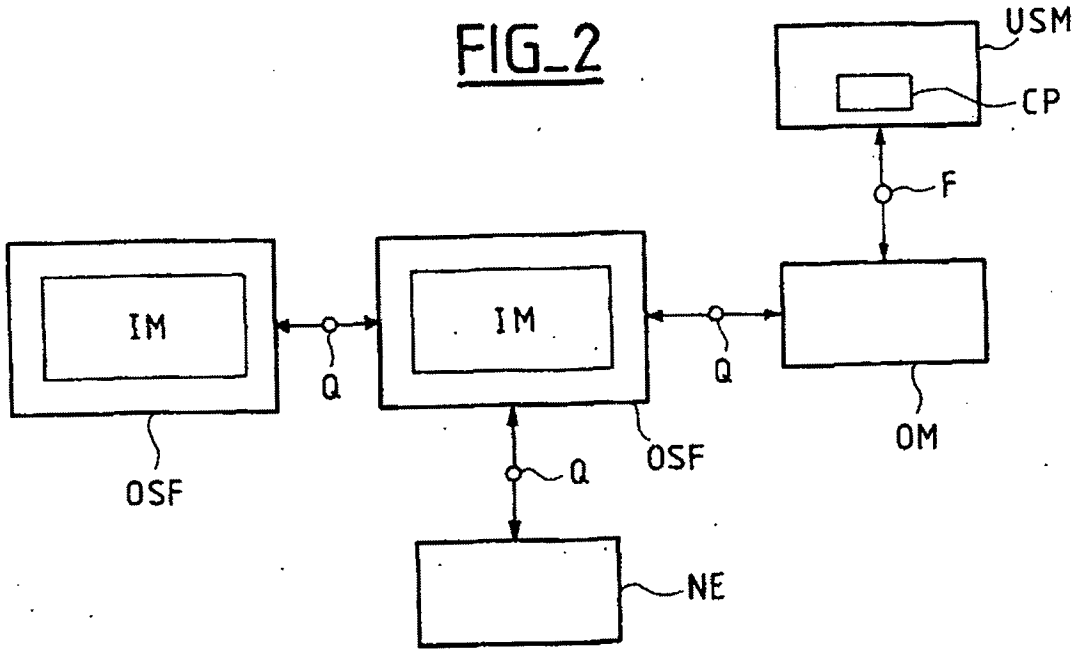

x
OSF
q3
f
x
OSF
f
WSF
g
q3
MF
f
f
q3
q3
qx
MF
qx
qx
QAF
NEF
QAF
NEF
m
m

FIG_2


USM
CP
F
IM
IM
Q
Q
OSF
OSF
Q
OM
NE

AUSTRALIA

Patents Act 1990

ORIGINAL
COMPLETE SPECIFICATION
STANDARD PATENT

Invention Title: A system for managing telecommunications network

The following statement is a full description of this invention, including the best method of performing it known to us:

A SYSTEM FOR MANAGING A TELECOMMUNICATIONS NETWORK

The invention relates to a system for managing a telecommunications network.

It is known that a telecommunications network is constituted by the assembly of hardware and of software enabling paying users to communicate. Such hardware naturally includes user telecommunications terminals which can equally well be stationary or mobile terminals. There are also systems for accessing the network, switching centers, and centers for managing the network.

The invention applies to any type of telecommunications network, whether stationary or mobile.

Attention is given below more particularly to centers for managing a telecommunications network, also referred to as the operation system (OS). These centers enable the operator of a telecommunications network to manage the network and to configure it.

It is known that a telecommunications network management center is structured as five functional blocks, F, A, C, P, and S, specifically for managing faults F, configuration C, information about payload A, performance (quality, throughput) P, and security S.

A management center does not operate in real time relative to the communications network itself. There is no need for the management center to penetrate into the network on each occasion that a telephone call needs to be set up. However, these centers serve to extract information from the network or to input information into the network each time it is necessary to take action for surveillance or reconfiguration, depending on the problem encountered.

Links between the management centers OS and the various elements of the telecommunications network have been standardized by the ITU. These recommendations are defined in a series known as M and a series known as X, where M relates to the practical aspects and X relates to communications protocols and implementation.

Mention can be made mainly of the ITU-T M3010 standard which describes a concept known as TMN: Telecommunications Management Network. The operational architecture of such TMN is shown in Figure 1. According to the standard, a TMN can include several types of operational assemblies, some of which are optional:

. OSF (Operation System Function)
. WSF (Work Station Function)
. MF (Mediation Function)
. QAF (Q Adaptor Functions)
. NEF (Network Element Function)

All these functions will not be described in detail since some of them are not within the scope of the present invention.

The management center proper is conventionally constituted by the OSF and WSF functions. The OSF functions. The management application proper is in the

OSF assembly and the operator interface and presentation function assemblies are in the WSF assembly.

All these functional assemblies can transfer information to and from each other via interfaces. According to the standard, interfaces of the f type link the functional assemblies of the WSF type to the functional assemblies of the MF and OSF types. Interfaces of the q3 type make it possible to link the functional assemblies of the OSF type to the functional assemblies of the OSF, MF, QAF and NF types. Interfaces of the qx type make it possible to link functional assemblies MF to functional assemblies of the MF, QAF and NF types.

Eventually, x, q and m interfaces make communications with the outside of the TMN possible from the OSF, WSF and QAF assemblies, respectively.

Interface q (also called "reference point q" is defined by a language for modelling the interface since it is dependent of each of the elements of the managed network. According to the standard, this description language is the GDMO language (Guideline for the Definition of Managed Objects). The ASN.1 language (Abstract Syntax Notation 1) can also be used for the definition of data.

For the f interface, the recommendations are general. No real specification is provided stating how the interface F should be implemented.

Thus, the state of the art often consists in basing the user interface functions (WSF) directly on the interfaces q.

Unfortunately, q interfaces are not designed to support the user presentation layers (operators) of WSF

functional assemblies. The q interface is designed for dialogs between management systems.

Basing operator interfaces directly on the q interface leads to the following drawbacks:

- The semantic distance between the definitions of objects at the q interface and their representation is very large, so the cost of developing such a function is very high. As a result, changing the type of representation is very expensive.

- The WSF function becomes totally dependent of the system. In other words, having the same implementation of the WSF function become common to a plurality of applications which cannot be linked by a q interface is not easily achievable.

The standard defining the ITU-T M3010 TMN (Telecommunication Management Network) architecture defines a presentation interface for network management systems known as the f interface. However, as already mentioned, that standard says little as to the formal definition of the interface.

Management systems based on TMN architecture do not implement the f interface. User interfaces are directly linked to the q interface which is described, as mentioned above in the GDMO/ASN.1 language, and thus with the above-mentioned drawbacks. In practice, it is necessary to develop as many USM user interface modules (for User Management System) implementing an OSF function as there are desired presentation layers with a q interface.

According to a first aspect of the present invention there is provided a telecommunications network management system comprising one or more network information management modules , and one or more user service modules , wherein the system includes a software architecture having an interface suitable for supporting one or more user presentation layers for a user services management module, and the software architecture includes a mediation layer between the interface supporting the user presentation layers, and the information management module.

In practice, an additional interface corresponding to the f interface of the TMN telecommunications management network is preferably introduced in the user service manager USM module (User Service Manager).

The interface is constructed on the basis of needs common to all of the presentation modes, its model is linked to the external representation of the entities managed by the system. A single software layer for mediation between the f interface and the q interface is provided and shared between all of the user presentation modules.

Other features and advantages of the invention will appear on reading the following description which is given by way of non-limiting example and with reference to the accompanying drawings, in which:

Figure 1, described above, is a general diagram illustrating the functional assemblies of a telecommunications management network (TMN);

Figure 2 is a general block diagram of a management system of the invention; and

Figure 3 is a detailed block diagram of the software architecture of the invention.

As shown in Figure 2, a network information management module IM1 can be linked to another network

information management module or to a network element NE via a reference point q (i.e. a q interface as defined above).

These two management modules IM1 and IM2 respectively implement tow functions OSF1 and OSF2 (arbitrarily shown as two bounding boxes.

The figure also shows a user interface module USM.

In accordance with the invention, and for the reasons mentioned above, it is proposed to fit the management system with a software architecture that includes an f interface suitable for supporting one or more user presentation layers CP of a user services management module USM.

The software architecture also includes a mediation layer OM between the f interface supporting the user presentation layers CP and the information management module IM1 which is linked to the user services management module USM.

In practice, the f interface corresponds to a standardized f interface of a TMN network. By way of example it can be introduced into the software module USM. The interface is constructed on the basis of the needs that are common to all of the presentation modes and its model is linked to the external presentation of the entities managed by the system.

The mediation layer OM between the f interface and the q interface is single and shared by all of the user presentation modules or "presentation handlers".

Figure 3 is a diagram showing the software architecture of the invention in greater detail. Elements already shown in Figure 2 can be found in this Figure 3.

The information from a q interface is, for instance, transported by the CMIP protocol (Common Management Information) and modelled using the language known as GDMO/ASN.1 which is a language from the telecommunications field, and the information is received by the mediation layer OM.

Level 1 of the mediation layer manages data interchange with the q interface.

Thereafter, levels 2 and 3 serve respectively to go from the QM model of data representation to the FM model, and from the FM model of data representation to the QM model. FM model means the data model used for performing the interchange of data via an f interface. Similarly, le QM model is the data model used for the q interface.

Level 4 defines the data representation FM model of the f interface. According to embodiments of the invention, this can be a representation of information based on the CORBA or CORBA-IDL languages (Interface Description Language) or on function calls in the C++ language.

Thus, the mediation layer OM, in addition to making the transformation of data representation models can make protocol translations.

For instance, it can translate between the CMIP protocol and the IIOP protocol or all of the protocols based on technologies of the CORBA type as well as those defined by the OMG (Open Management Group).

To this end, the mediation layer OM concatenates the inheritance levels of the GDMO language and transforms ASN.1 types into base type, and vice versa.

The f interface preferably supports a plurality of types of user presentation layer.

In one embodiment, the user presentation layers can be integrated in the mediation layer OM.

In another embodiment, the user presentation layers can be integrated in the user service management model USM, as shown in Figure 3.

In the embodiment shown, the f interface supports the following user presentation layers:

- a direct graphics interface G;
- a script language S enabling users to describe their own macro-instructions FS1 or macro-instructions stored in files FS2 via a user interface IU; and
- an access AR to Internet or Intranet computer networks or to any client application via the IIOP communications protocol.

The F interface also supports a presentation layer such as an agenda function A.

A link to a journalisation module F_Log, can be added to the mediation layer OM, the aim of this module being making it possible to store the translations carried out by this layer.

The above-described software architecture makes it possible to provide open modules for user services management USM.

Claims

1 A telecommunications network management system comprising one or more network information management modules , and one or more user service modules , wherein the system includes a software architecture having an interface suitable for supporting one or more user presentation layers for a user services management module, and the software architecture includes a mediation layer between the interface supporting the user presentation layers, and the information management module.

2 A network management system according to claim 1, wherein the mediation layer enables interchanges to be performed between a CMIP protocol supporting a representation of information based on the GDMO/ASN.1 language, and a protocol based on the CORBA technology supporting a representation of information based on the CORBA or IDL languages.

3 A network management system according to claim 2, wherein the mediation layer serves to concatenate the inheritance levels of the GDMO language and to transform ASN.1 types into base type, and vice versa.

4 A network management system according to any one of the preceding claims wherein the interface supports one or more types of user presentation layers.

5 A network management system according to any one of the preceding claims , wherein the user presentation layers are integrated in the mediation layer.

6 A network management system according to any one of the preceding claims , wherein the user presentation layers are integrated in the user services management module.

7 A network management system according to any one of the preceding claims, wherein the interface supports:

- a direct graphics interface;
- a script language enabling users to describe their own macro-instructions; and
- an access to computer networks via the IIOP protocol.

8 A network management system substantially as hereinbefore described with reference to figure 2 or 3 of the accompanying drawings.

Dated this 26th day of August 1999

Alcatel

5 **by its attorneys**

Freehills Patent Attorneys

FIG_1

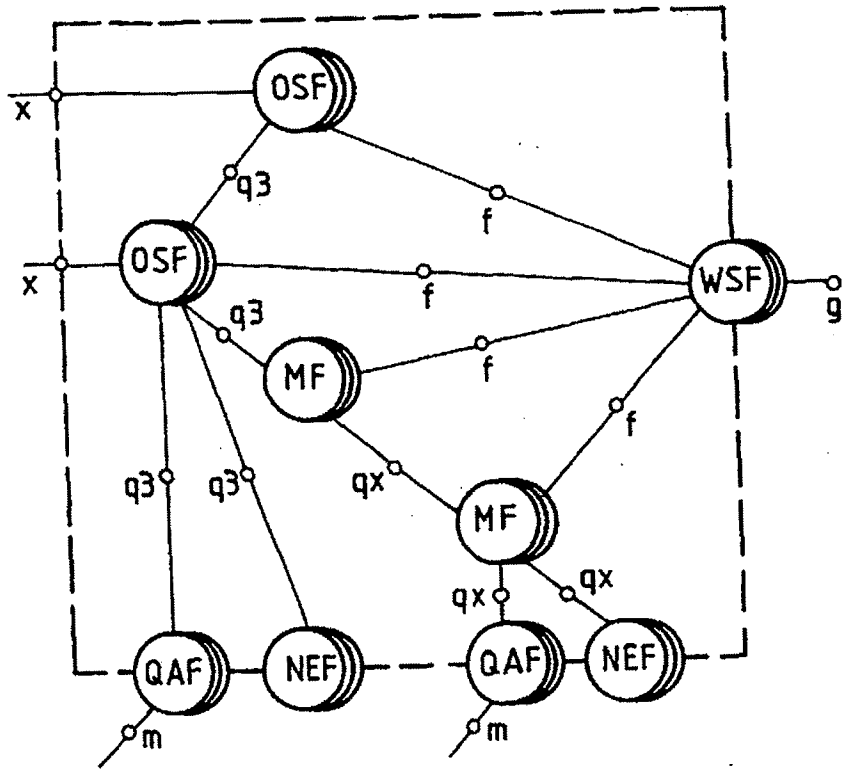

x
OSF
q3
f
x
OSF
f
WSF
g
q3
MF
f
f
q3
q3
qx
MF
qx
qx
QAF
NEF
QAF
NEF
m
m

FIG_2

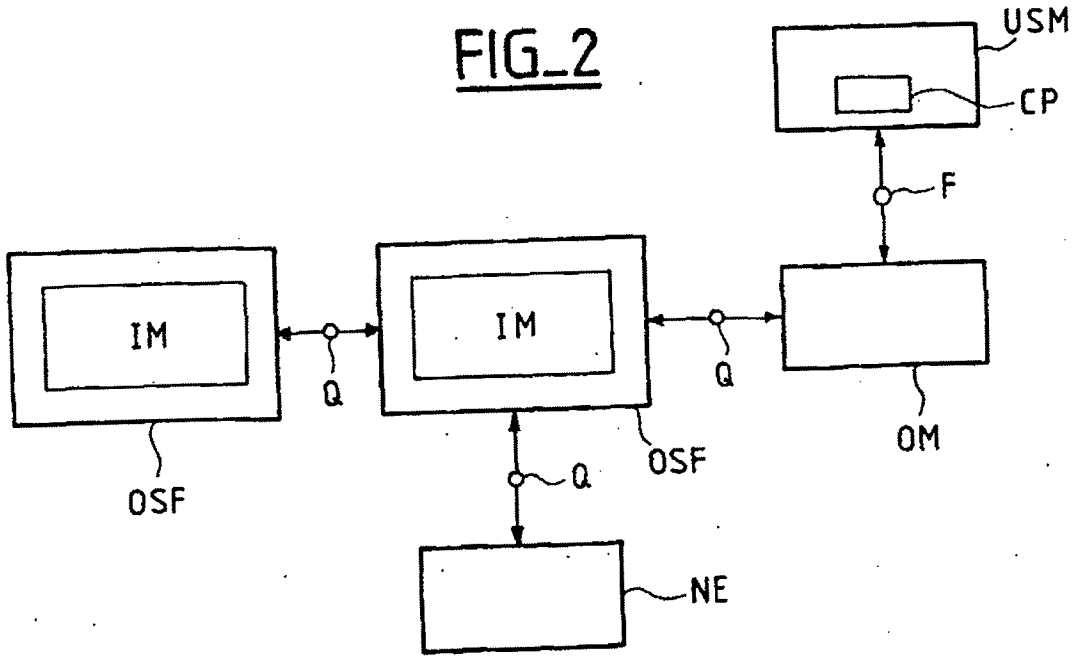
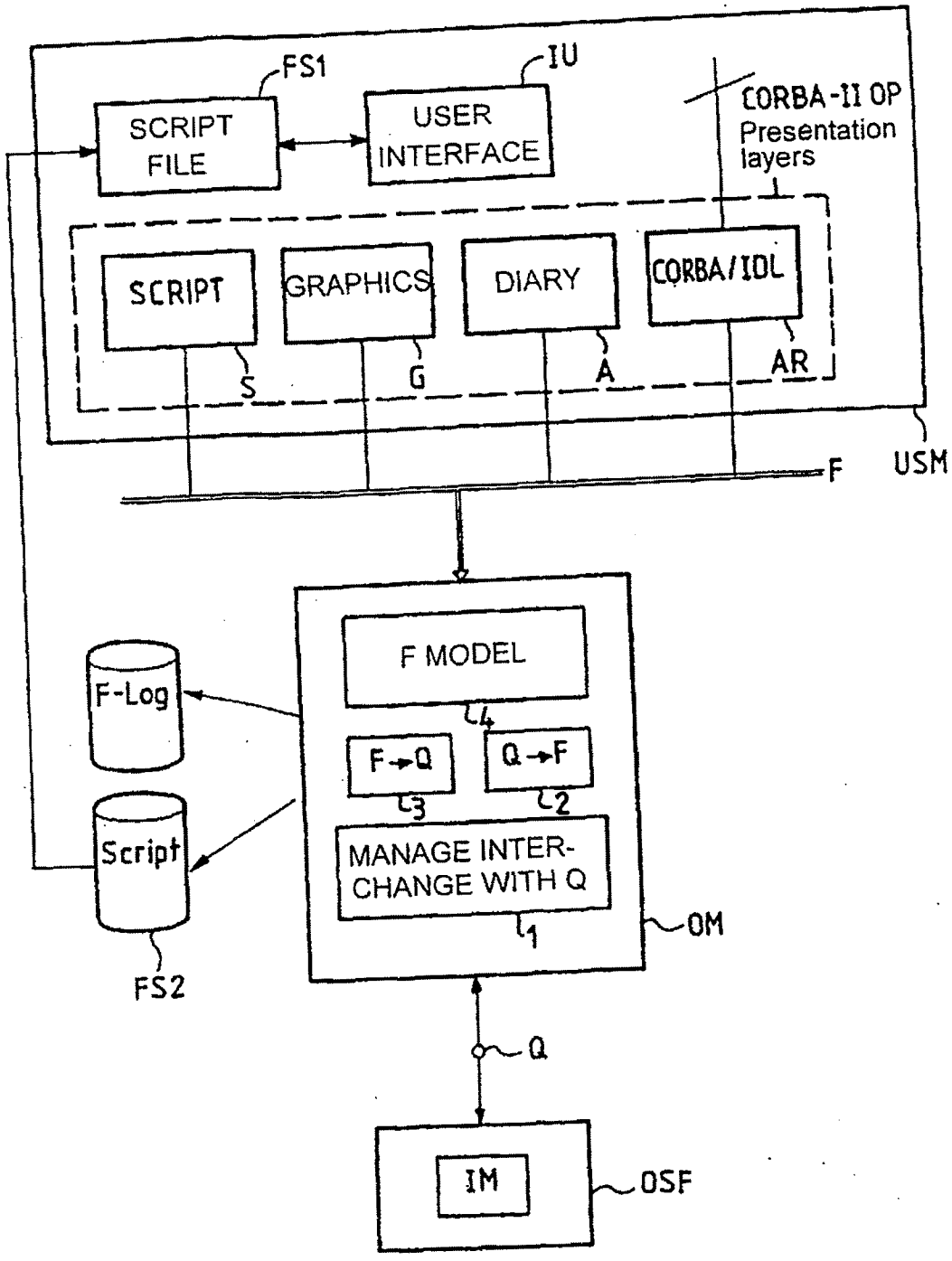

USM
CP
F
IM
IM
Q
Q
OSF
OSF
OM
Q
NE

FIG_3


FS1
IU
SCRIPT FILE
USER INTERFACE
CORBA-II OP Presentation layers
SCRIPT
GRAPHICS
DIARY
CORBA/IDL
S
G
A
AR
F
USM
F MODEL
F-Log
F→Q
Q→F
Script
MANAGE INTER-CHANGE WITH Q
OM
FS2
Q
IM
OSF

Citation 1

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－124986
（P2003－124986A）
(43)公開日　平成15年４月25日(2003.4.25)

(51)Int.Cl.[7]	識別記号	FI		テーマコード*(参考)
H04L 12/56	200	H04L 12/56	200F	5K030
12/46		12/46	V	5K033
H04M 3/00		H04M 3/00	D	5K051

審査請求　未請求　請求項の数５　ＯＬ　（全 33 頁）

(21)出願番号　特願2001－320913(P2001－320913)

(22)出願日　平成13年10月18日(2001.10.18)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　張　大維
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　新井　敏正
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

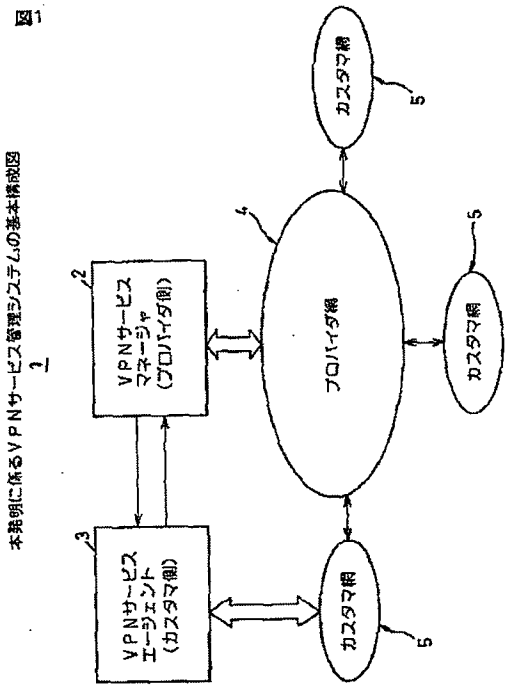
(74)代理人　100077517
弁理士　石田　敬　（外４名）

最終頁に続く

(54)【発明の名称】　ＶＰＮサービス管理システム、ＶＰＮサービスマネージャ及びＶＰＮサービスエージェント

(57)【要約】
【課題】　迅速かつ簡単に、カスタマがＶＰＮサービス条件の変更を行うことのできるＶＰＮサービス管理システムを提供する。
【解決手段】　カスタマ網５と、プロバイダ網４と、を備える通信網に対しＶＰＮサービスの管理を行うためのＶＰＮサービス管理システムであり、プロバイダ網４に対してＶＰＮサービスの管理を行うＶＰＮサービスマネージャ２と、カスタマ網５に対してＶＰＮサービスの管理を行うＶＰＮサービスエージェント３と、を有し、ＶＰＮサービスマネージャ２は、ＶＰＮサービスエージェント３と連携し、カスタマ網５の運用状況に応じて、ＶＰＮサービス条件をリアルタイムに変更するように構成する。

図1



1

【特許請求の範囲】

【請求項１】　カスタマを収容するカスタマ網と、該カスタマにＶＰＮサービスを提供するプロバイダによって構築され該カスタマ網に連結するプロバイダ網と、を備える通信網に対し該ＶＰＮサービスの管理を行うためのＶＰＮサービス管理システムであって、

前記プロバイダ網に対して前記ＶＰＮサービスの管理を行うＶＰＮサービスマネージャと、

前記カスタマ網に対して前記ＶＰＮサービスの管理を行うＶＰＮサービスエージェントと、を有し、

前記ＶＰＮサービスマネージャは前記ＶＰＮサービスエージェントと連携し、該ＶＰＮサービスエージェントの管理下にある前記カスタマ網の運用状況に応じて、提供すべき前記ＶＰＮサービスのＶＰＮサービス条件をリアルタイムに変更することを特徴とするＶＰＮサービス管理システム。

【請求項２】　前記プロバイダ側に前記ＶＰＮサービスマネージャと協働するプロバイダ網管理システムをさらに有し、該プロバイダ網管理システムは、前記カスタマ網内に前記プロバイダ網との接続用に配備されるカスタマエッジをも含めて該プロバイダ網を管理することを特徴とする請求項１に記載のＶＰＮサービス管理システム。

【請求項３】　前記カスタマ側に前記ＶＰＮサービスエージェントと協働すると共に前記カスタマ網を管理するカスタマ網管理システムをさらに有し、該カスタマ網管理システムは、前記カスタマエッジを監視しかつ前記プロバイダ網側との通信を行うことを特徴とする請求項２に記載のＶＰＮサービス管理システム。

【請求項４】　カスタマを収容するカスタマ網と、該カスタマにＶＰＮサービスを提供するプロバイダによって構築され該カスタマ網に連結するプロバイダ網と、を備える通信網に対し該ＶＰＮサービスの管理を行うためのＶＰＮサービス管理システムを構成するＶＰＮサービスマネージャであって、

前記プロバイダ網に対して前記ＶＰＮサービスの管理を行うと共に、

前記カスタマ網に対して前記ＶＰＮサービスの管理を行うＶＰＮサービスエージェントと連携して、該ＶＰＮサービスエージェントの管理下にある前記カスタマ網の運用状況に応じて、前記ＶＰＮサービス管理システムが提供すべき前記ＶＰＮサービスのＶＰＮサービス条件をリアルタイムに変更することを特徴とするＶＰＮサービスマネージャ。

【請求項５】　カスタマを収容するカスタマ網と、該カスタマにＶＰＮサービスを提供するプロバイダによって構築され該カスタマ網に連結するプロバイダ網と、を備える通信網に対し該ＶＰＮサービスの管理を行うためのＶＰＮサービス管理システムを構成するＶＰＮサービスエージェントであって、

2

前記カスタマ網に対して前記ＶＰＮサービスの管理を行うと共に、

前記プロバイダ網に対して前記ＶＰＮサービスの管理を行うＶＰＮサービスマネージャと連携して、管理下にある前記カスタマ網の運用状況に応じて、前記ＶＰＮサービス管理システムが提供すべき前記ＶＰＮサービスのＶＰＮサービス条件をリアルタイムに変更することを特徴とするＶＰＮサービスエージェント。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＶＰＮサービス管理システムと、そのシステムを構成するＶＰＮサービスマネージャおよびＶＰＮサービスエージェントに関する。

【０００２】特に、本発明は、インターネットサービスプロバイダ（ＩＳＰ）やアプリケーションサービスプロバイダ（ＡＳＰ）、あるいは複数の事業所拠点を有しこれらの拠点間でエクストラネットワークを運営する企業等が、広域な事業運営を進めるために、第一種通信事業者が提供する仮想専用線網（ＶＰＮ：ＶｉｒｔｕａｌＰｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）を使用する場合における、ＶＰＮサービスの運用形態に関する。なお以下の説明では、ＶＰＮサービスを提供する通信事業者（キャリア）をプロバイダと称し、ＶＰＮサービスを利用するＩＳＰ，ＡＳＰ、企業等を総称してカスタマと称する。また、プロバイダおよびカスタマが運用管理するネットワーク（網）については、それぞれプロバイダ網およびカスタマ網と呼ぶ。

【０００３】

【従来の技術】オンラインバンキングやインターネット電話等、インターネット上において各種の新しいサービスが続々と登場するのに伴い、インターネットをビジネス上で利用する主としてカスタマにおいて、より高速でかつコストの安い高品質な通信環境を求める声が高まってきている。さらに、このような通信環境のもとではネットワーク・セキュリティの確保が不可欠になってきており、インターネットを仮想的に専用線のように利用することができるＩＰ－ＶＰＮ（ＩＰ－ＶｉｒｔｕａｌＰｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）が、現在注目されている。そしてプロバイダは、かかるＩＰ－ＶＰＮを用いた高品質通信サービスを、カスタマのニーズに合わせて提供し始めている。

【０００４】カスタマ側は、このＩＰ－ＶＰＮ高品質通信サービスを利用する場合、予めプロバイダとの契約時に、希望する接続拠点、保証帯域幅、ＱｏＳ、ポリシー、データロス（パケットロス）、遅延時間等についての条件を指定し、その契約条件に応じた一定のサービス使用料を例えば月単位で、プロバイダ側に支払う。この場合、カスタマ側は希望すれば、通常は有料で、そのＩＰ－ＶＰＮ高品質通信サービス（以下、単にＶＰＮサー

ビスとも称す）の契約条件を随時変更することができる。

【０００５】従来、そのような契約条件の変更にあたっては、（ｉ）カスタマあるいはその代行者が、書面やＦＡＸ、電話等の手段を用いて該変更の申し込み、プロバイダのサービスオーダ手配を経た後に、（ii）プロバイダのオペレータが、該変更に必要なＶＰＮサービス条件の設定を行う。このような手順を経ることにより、希望のサービスをカスタマに提供できる環境が整う。

【０００６】

【発明が解決しようとする課題】上記のような、カスタマとプロバイダとの間での契約条件の変更手続きにおいては、従来、上記の申込みから変更後のサービスを開始できるまでに、所定の期間、例えば数日から数週間を必要とする、という問題があった。このため、以下の使用例のような、突発的あるいは不定期的にカスタマ側で発生する、ＶＰＮサービス利用条件の変更要求に対して、タイムリーに対応できない、という不便があった。

【０００７】１）企業での使用例：企業の社長による、年頭のあいさつあるいは中期ビジョンの発表を、企業内イントラネットを介し、全事業所拠点の全社員に対して一斉に放映したい。

【０００８】２）ＩＳＰでの使用例：新サービスの業務開始に向けて、既存のＶＰＮ網の帯域幅を、一斉に倍増したい。

【０００９】３）ＡＳＰでの使用例：Ｗｅｂチケット販売サービスを実施するとき、例えば人気グループのチケット発売期間中のみ、その申込みの殺到に備えたい。

【００１０】また、カスタマ網およびプロバイダ網のそれぞれのネットワーク管理システムが、相互に完全に独立して構成されているため、該カスタマ網内で検出された、トラヒックや通信パケット量の増大あるいはインターネットアクセス応答性能の劣化といった、ＶＰＮサービス条件の急変に対し、ＶＰＮサービスの品質条件や利用条件を簡単には変更することができない、という問題があった。

【００１１】また、プロバイダ側の立場からは、ＶＰＮサービスを提供するための、プロバイダ網内の設備については、その品質条件を検証することができるが、しかし他方、カスタマ網内に配備されるカスタマエッジ（ＣＥ）については、その機種の選定から管理まで全てカスタマ側に委ねられているため、カスタマエッジ（ＣＥ）側の機種およびその仕様が起因して後日、変更される等に、契約時に締結したサービス品質の合意（ＳＬＡ：Ｓｅｒｖｉｃｅ　Ｌｅｖｅｌ　Ａｇｒｅｅｍｅｎｔ）を遵守することが困難になる、という問題があった。

【００１２】したがって本発明は、上記諸問題点に鑑み、

１）カスタマとプロバイダとの間での契約条件を変更したいというカスタマ側の要求に対し、迅速に応えることができ、

２）ＩＰ－ＶＰＮサービス等のＶＰＮサービスの品質条件や利用条件を簡単に変更することができ、

３）カスタマとプロバイダとの間での契約によって締結した、サービス品質の合意を常に遵守することができる、ＩＰ－ＶＰＮサービス等のＶＰＮサービス管理システムを実現することを目的とするものである。

【００１３】

【課題を解決するための手段】図１は本発明に係るＶＰＮサービス管理システムの基本構成図である。

【００１４】本図において、参照番号１はＶＰＮサービス管理システムを示す。これは、カスタマを収容するカスタマ網５と、このカスタマにＶＰＮサービスを提供するプロバイダによって構築されカスタマ網５に連結するプロバイダ網４と、を備える通信網に対しＶＰＮサービスの管理を行うためのＶＰＮサービス管理システムである。該システム１は、プロバイダ網４に対してＶＰＮサービスの管理を行うＶＰＮサービスマネージャ２と、カスタマ網５に対してＶＰＮサービスの管理を行うＶＰＮサービスエージェント３と、を少なくとも有する。

【００１５】ここにＶＰＮサービスマネージャ２はＶＰＮサービスエージェント３と連携し、ＶＰＮサービスエージェント３の管理下にあるカスタマ網５の運用状況に応じて、システム１が提供すべきＶＰＮサービスのＶＰＮサービス条件をリアルタイムに変更するように構成する。

【００１６】上記の構成によって、従来における前述したＶＰＮサービスの契約の変更を迅速に行えないという第１の問題と、ＶＰＮサービスの品質条件あるいは利用条件（ＶＰＮサービス条件）を簡単には変更できないという第２の問題と、サービス品質の合意を常に遵守することが困難であるという第３の問題と、を解決することができる。以下、具体的に詳しく説明する。

【００１７】

【発明の実施の形態】本発明の理解を容易にするために、まず本発明の全体を説明して本発明の意図するところを明らかにしてから、次いで本発明の各構成要素について個々に説明する。

【００１８】図２は従来の典型的なＶＰＮサービスネットワークを図解的に示す図である。

【００１９】本図において、参照番号６はキャリア網であり、一般的な専用線サービスでのキャリアの管理範囲を表す。

【００２０】このキャリア網６の配下には、複数のカスタマ網５が配設される。本図の例では、カスタマＡが４つの拠点に有するカスタマＡ網－１，２，３および４が示されている。

【００２１】上記キャリア網６を中心として、これらのカスタマ網５の間でＶＰＮサービスネットワークを構築するために、図示するカスタマＡ用専用線網が形成され

る。このカスタマA用専用線網は、キャリア網６内のプロバイダエッジPE（Ｐｒｏｖｉｄｅｒ　Ｅｄｇｅ）ならびにプロバイダコアルータPCR（Ｐｒｏｖｉｄｅｒ　Ｃｏｒｅ　Ｒｏｕｔｅｒ）およびカスタマ網５内のカスタマエッジCE（Ｃｕｓｔｏｍｅｒ　Ｅｄｇｅ）ならびにカスタマルータCR（ＣｕｓｔｏｍｅｒＲｏｕｔｅｒ）を経由して、各カスタマ相互間に形成される。これに対して本発明のＶＰＮサービスネットワークは次のように構築される。

【００２２】図３は本発明により形成されるＶＰＮサービスネットワークを図解的に示す図であり、図２の構成をベースにして表している。なお、全図を通じて同様の構成要素には同一の参照番号または記号を付して示す。

【００２３】図２と図３を比べると、図２では各カスタマ網５の管理下にあったカスタマエッジCEが、図３ではキャリア網側の監理下にも置かれる点で、両者間に相違がある。すなわち、本発明のプロバイダ網４では、本来のキャリア網の管理範囲がカスタマ側迄拡大している。これにより、カスタマエッジを通してＶＰＮサービス条件を制御することが可能となる。一方、このためにプロバイダ側では図示するプロバイダ網管理システム（Ｐ－NMS：Ｐｒｏｖｉｄｅｒ　ＮｅｔｗｏｒｋＭａｎａｇｅｍｅｎｔ　Ｓｙｓｔｅｍ）１２が有用な管理手段となり、また、カスタマ側では図示するカスタマ網管理システム（Ｃ－NMS：Ｃｕｓｔｏｍｅｒ　Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ　Ｓｙｓｔｅｍ）が有用な管理手段となる。なお、Ｃ－NMSは上記のカスタマA網－１，２，３および４に対して少なくとも１つあればよい。

【００２４】図３に示すＶＰＮサービスネットワークによれば、次の〔１〕～〔３〕に示すビジネスメリットが期待される。

【００２５】まずプロバイダ側からの視点によれば、

〔１〕カスタマエッジCEも含めたカスタマＶＰＮ網の２４時間監視サービス（アウトソーシング）を実現できる。

【００２６】〔２〕ＶＰＮサービスとそのＶＰＮサービス条件の均質化を図ることができ、その結果、カスタマエッジCEについてベンダ機種毎に依存した仕様への対応が不要となる。

【００２７】またベンダ側からの視点によれば、上記〔１〕および〔２〕に加えて、〔３〕１つのベンダが、１つのプロバイダに対しこのプロバイダとの契約のもとに、そのベンダ独自のカスタマエッジ（CE）と、プロバイダ管理システム（Ｐ－NMS）およびカスタマ管理システム（Ｃ－NMS）と、を継続的に供給することができる。

【００２８】上記〔１〕、〔２〕および〔３〕に示すビジネスメリットをもたらすＶＰＮサービス管理システムを次に説明する。

【００２９】図４は本発明に係るＶＰＮサービス管理システムの全体を表す図である。本図は、前述した図１のシステム構成を、現実に即して、具体例として表す図である。

【００３０】図３において、図１に示すＶＰＮサービスマネージャ２は、プロバイダ網管理センター７内に収容されている。また該センター７内には既述のプロバイダ網管理システム（Ｐ－NMS）１２も収容されている。なお本図では、一例として２つのシステムがＰ－NMS１およびＰ－NMS２として表わされている。種々のビジネス用途を考慮したものである。

【００３１】一方、図３において、図１に示すＶＰＮサービスエージェント３は、カスタマ網管理センター８内に収容されている。また該センター８内には既述のカスタマ網管理システム（Ｃ－NMS）１３も収容されている。

【００３２】以上の構成要素と、プロバイダ網４およびカスタマ網５と、が連携して本発明に係るＶＰＮサービス管理システム１が構築される。

【００３３】このＶＰＮサービス管理システム１において特に注目すべき点は、下記の３つの要件＜１＞、＜２＞および＜３＞を満足できることである。これらの３つの要件は従来のＶＰＮサービスのもとでは満足することができなかった。

【００３４】また、下記の３つの要件＜１＞、＜２＞および＜３＞が満足されることによって、既述した３つのカスタマ（例えば企業ユーザ）側の要求１）、２）および３）が実現可能となる。すなわち

１）企業での使用例：企業の社長による、年頭のあいさつあるいは中期ビジョンの発表を、企業内イントラネットを介し、全事業所拠点の全社員に対して一斉に放映したい、

２）ＩＳＰでの使用例：新サービスの業務開始に向けて、既存のＶＰＮ網の帯域幅を、一斉に倍増したい、

３）ＡＳＰでの使用例：Ｗｅｂチケット販売サービスを実施するとき、例えば人気グループのチケット発売期間中のみ、その申込みの殺到に備えたい、という要求である。

【００３５】ここに上記の３つの要件＜１＞、＜２＞および＜３＞を示すと、次のとおりである。すなわち、本発明のＶＰＮサービス管理システム１によれば、＜１＞プロバイダ側から提供されるＶＰＮサービス条件（ＶＰＮサービスの品質条件や利用条件）を変更することが、カスタマ側（例えば企業ユーザ側）自身によって即座に行えること、＜２＞カスタマ網５でのトラヒック特性やＶＰＮの使用形態に応じて、自動的にあるいは時間指定で、上記ＶＰＮサービス条件を簡単に変更できること、＜３＞カスタマがプロバイダと契約したＶＰＮを用いて（例えば、インーバンド（Ｉｎ－Ｂａｎｄ）通信形態を使用して）、カスタマ（例えば企業ユーザ）が上記ＶＰ

Ｎサービス条件の設定を制御できること、といった要件が満足される。

【００３６】ここで再び図４を参照すると、上記要件＜１＞、＜２＞および＜３＞にそれぞれ相当する処理の流れが、本図中のルートＲ＜１＞、Ｒ＜２＞およびＲ＜３＞として示されている。

【００３７】ルートＲ＜１＞では、ＶＰＮサービスマネージャ２がＶＰＮサービスエージェント３に対して、ＶＰＮサービスメニューを提供する。このメニューにはカスタマに提供可能な各種のＶＰＮサービスが表示されている。

【００３８】またルートＲ＜１＞では、ＶＰＮサービスエージェント３の配下のカスタマ網５のＶＰＮ使用状況を勘案しかつ上記メニューを参照して、希望するＶＰＮサービスをＶＰＮサービスマネージャ２に対して要求する。

【００３９】ルートＲ＜２＞においては、ＶＰＮサービスエージェント３は、Ｃ－ＮＭＳ１３を介して、配下のカスタマ網５におけるトラヒック特性やＶＰＮの使用形態に関する情報を収集し、上記ルートＲ＜１＞における図示のＶＰＮサービス要求を生成する。

【００４０】ルートＲ＜３＞においては、上記の収集したトラヒック特性やＶＰＮの使用形態に関する情報を、実際にプロバイダ側において反映させる。すなわちその情報をプロバイダ側に伝送する。この伝送はＣ－ＮＭＳ１３からカスタマエッジＣＥを経由して行うことにより、契約中のＶＰＮをインーバンドに使用する。

【００４１】〔第１の態様〕上記要件＜１＞、＜２＞および＜３＞を満足するＶＰＮサービス管理システム１について、その細部を具体的に説明する。

【００４２】図５は本発明に係るＶＰＮサービス管理システム１の基本構成を示す図である。したがって本図の構成は殆ど図４の構成の中に含まれる。

【００４３】本図において注目すべき構成は、次のとおりである。

【００４４】システム１は、プロバイダ側にＶＰＮサービスマネージャ２と協働するプロバイダ網管理システム（Ｐ－ＮＭＳ）１２をさらに有し、このプロバイダ網管理システム１２は、カスタマ網５内にプロバイダ網４との接続用に配備されるカスタマエッジＣＥをも含めて、プロバイダ網４を管理する。

【００４５】システム１は、ＶＰＮサービスマネージャ２とＶＰＮサービスエージェント３の他には、最低限プロバイダ網管理システム（Ｐ－ＮＭＳ）１２を備えていればよい。しかしさらに種々の機能をもたせるには、図５には示していないが既述のカスタマ網管理システム（Ｃ－ＮＭＳ）１３を設置するのが好ましい。すなわちシステム１は、カスタマ側にＶＰＮサービスエージェント３と協働すると共にカスタマ網４を管理するカスタマ網管理システム（Ｃ－ＮＭＳ）１３をさらに有し、このカスタマ網管理システム１３は、カスタマエッジＣＥを監視しかつプロバイダ網４側との通信を行う。

【００４６】図５の例によると、ＶＰＮサービスマネージャ２は、カスタマＡにカスタマＡ網用のＩＰ－ＶＰＮ監視ビューを、既述のＶＰＮサービスメニューとして提示する。カスタマＡはこのＩＰ－ＶＰＮ監視ビューに従って所望のＩＰ－ＶＰＮサービスを、ＶＰＮサービスエージェント３よりプロバイダ側に要求する。なお、本図では、カスタマＡ網と連係する他のカスタマＡ網（図３参照）についてはその記載を省略している。該他のカスタマＡ網は、例えば図示するカスタマＡ網が東京に所在するとすれば、北海道、名古屋、大阪、九州等にそれぞれ所在するという網構成が考えられる。上記図５の構成をさらに具体的に説明する。

【００４７】図６は図５の構成を具体例によって示す図である。

【００４８】本図の概略構成を説明する。なお、本図中、Ｅ１，Ｅ２，Ｅ３…は各種のイベントを表わすが、これらのイベントについては後述の図１０および図１１を参照して詳しく説明する。

【００４９】図６においてＰ－ｉｐは、ＶＰＮサービスのプロバイダ側ＩＰ網である。Ｃ－ｉｐ１，Ｃ－ｉｐ２は、ＶＰＮサービスのカスタマ側のＩＰ網であり、Ｐ－ｉｐに接続されている。このＰ－ｉｐには複数のＶＰＮサービスのカスタマ側ＩＰ網が接続されている。ここに、上記のＶＰＮサービスとは、複数の部分的カスタマＩＰ網について、プロバイダ側ＩＰ網が各カスタマＩＰ網間の情報を無加工で中継することにより、各カスタマＩＰ網から成る全体として１つの仮想的カスタマＩＰ網を実現する、既存技術に基づくサービスのことである。

【００５０】カスタマエッジＣＥは、各ＶＰＮサービスのカスタマＩＰ網と、ＶＰＮサービスのプロバイダＩＰ網とを接続するための各ＶＰＮサービスのカスタマ側のＩＰ装置である。またＰＥは、そのＣＥと接続する、ＶＰＮサービスのプロバイダ側ＩＰ装置である。

【００５１】プロバイダ網管理システムＰ－ＮＭＳ１２は、プロバイダ側ＩＰ装置であってＩＰ網の監視制御装置である。このＰ－ＮＭＳ１２は、プロバイダＩＰ装置およびＩＰ網の運行状況の監視と制御とを行う。

【００５２】カスタマ網管理システムＣ－ＮＭＳ１３は、カスタマ側ＩＰ装置であってＩＰ網の監視制御装置である。このＣ－ＮＭＳ１３は、カスタマＩＰ網の運行状況の監視と制御とを行う。

【００５３】これらのＰ－ＮＭＳ１２およびＣ－ＮＭＳ１３については、管理されるべきＩＰ装置とＩＰ網の規模、地理的条件や運用条件等により、任意の数が設置される場合がある。ここにＣ－ＮＭＳ１３は、ＣＥの監視と制御が可能であり、また、Ｐ－ＮＭＳ１２も、Ｃ－ＮＭＳ１３経由もしくはＰＥ経由で、ＣＥの監視と制御が可能である。

9

【００５４】本発明では、Ｃ－ｉｐ網上に設置されるＣＥに対してＶＰＮサービスの制御を可能とするＶＰＮサービスマネージャ２を、Ｐ－ＮＭＳ１２に配置する。

【００５５】またカスタマ側ＶＰＮサービス運用者が、ＶＰＮサービスマネージャ２に遠隔より制御できるための、ＶＰＮサービスエージェント３をＣ－ＮＭＳ１３に配置する。

【００５６】上記ＶＰＮサービスマネージャ２およびＶＰＮサービスエージェント３は、ＶＰＮサービス条件テーブルを両者間に介在させて、相互間の連携を図る。このテーブルについて以下に説明する。

【００５７】図７はＶＰＮサービス条件テーブルを図解的に表す図である。

【００５８】ＶＰＮサービスマネージャ２は、ＶＰＮサービスに関するサービスメニューを、本図のＶＰＮサービス条件テーブル１４として、ＶＰＮサービスエージェント３に提供する。カスタマ側にてＶＰＮサービス条件の変更要求が発生したとき、ＶＰＮサービスエージェント３はそのサービスメニューを介してその変更要求をＶＰＮサービスマネージャ２に送信し、ＶＰＮサービスマネージャ２は、プロバイダ網管理システム１２を介して、その変更要求をプロバイダ網４に反映させる。

【００５９】例えば、図６のＰ－ｉｐ網上もしくはＰ－ＮＭＳ１２に、このＶＰＮサービス条件テーブル１４が配置される。このＶＰＮサービス条件テーブル１４には、ＶＰＮサービスカスタマの識別子および当該カスタマに割り当てられているＶＰＮ識別子と、ＶＰＮの両端点（端点Ａ～端点Ｚ）であって当該カスタマ先に設置されているカスタマエッジＣＥの識別のためのＣＥ識別子と、ＶＰＮサービスカスタマが変更することのできるＶＰＮサービス条件項目一覧と、各ＶＰＮサービス条件項目毎に対応して現在設定されている現在の値と、ＶＰＮサービス条件値として許容される許容最大／最小値およびその設定幅（使用する帯域幅）と、が保持される。これらのＶＰＮサービス条件項目および許容される値の範囲は、カスタマとプロバイダとの間でＶＰＮサービス契約時に規定される場合もあるし、また、ＶＰＮサービスの状況またはＩＰ網の状態に応じてＶＰＮサービス条件項目が追加・削除される場合もある。なおこれらＶＰＮサービス条件項目は、ＶＰＮサービスを実現する技術仕様毎に異なる場合がある。これについて若干補足すると、大規模災害時には上記帯域の確保の指定はできなくなる。また帯域指定というＶＰＮサービス条件が削除されるか、または逆に、無線や衛星等の専用回線を用いて優先的に帯域確保ができる、専用回線経由というＶＰＮサービス条件を追加することができる。

【００６０】上記のようなＶＰＮサービス条件テーブル１４を介在させて、ＶＰＮサービスマネージャ２とＶＰＮサービスエージェント３とが相互に連携する。この連携のために、これらＶＰＮサービスマネージャ２とＶＰＮサービスエージェント３とがそれぞれ備えるべき手段（機能）を次に説明する。

10

【００６１】図８はＶＰＮサービスマネージャ２が有する機能を表す図であり、図９はＶＰＮサービスエージェント３が有する機能を表す図である。

【００６２】図８を参照すると、ＶＰＮサービスマネージャ２は、ＶＰＮサービスエージェント３からＶＰＮサービス条件（図７）を変更するオーダが発生したときこれを受信して、このオーダに係る変更ＶＰＮサービス条件を出力するＶＰＮサービスオーダ制御手段２１と、そのオーダが発生したとき、当該カスタマ網５に付与されている現ＶＰＮサービス条件を、ＶＰＮサービス条件テーブル（図７）から検索するＶＰＮサービス条件手段２２と、上記の変更ＶＰＮサービス条件が上記の現ＶＰＮサービス条件から超える範囲が許容範囲か否か判定するＶＰＮサービス条件判定手段２３と、上記の判定の結果が「可」であるとき、上記の現ＶＰＮサービス条件を上記の変更ＶＰＮサービス条件に設定し直すＶＰＮサービス条件設定手段２４と、上記の設定し直されたＶＰＮサービス条件に基づきカスタマエッジＣＥを制御するカスタマエッジ制御手段２５と、を備えている。

【００６３】この手段２５により、プロバイダ側ＶＰＮサービス運用者は、カスタマエッジＣＥのＶＰＮサービス制御が可能となる。

【００６４】さらに説明を補足すると、ＶＰＮサービスオーダ制御手段２１は、ＶＰＮサービスエージェント３からＶＰＮサービス条件を変更するオーダ（ＶＰＮサービスオーダ）を受信する。当該オーダに含まれるカスタマ識別子およびＶＰＮ識別子に基づき、同様に当該オーダに含まれる個々のＶＰＮサービス条件および値を、ＶＰＮサービス条件判定手段２３に渡す。

【００６５】サービス条件判定手段２３の判定結果が「可」であれば、ＶＰＮサービス条件設定手段２４を用いて、ＶＰＮサービス条件テーブル１４の現在の値を変更する。

【００６６】その後、ＶＰＮサービス条件および値を、ＣＥに対応した制御情報に変換したのち、ＣＥ制御手段２５に対して制御情報を送信する。さらにＶＰＮサービス条件判定手段２３の判定結果と、ＣＥ制御手段２５による制御の結果と、に基づき、ＶＰＮサービスエージェント３にその結果を応答する。

【００６７】ＶＰＮサービス条件検索手段２２は、カスタマ識別子およびＶＰＮ識別子に対するＶＰＮサービス条件テーブル１４の内容を取出す。

【００６８】ＶＰＮサービス条件判定手段２３は、カスタマ識別子およびＶＰＮ識別子に基づき、ＶＰＮサービス条件変更オーダに含まれる個々のＶＰＮサービス条件および値について、ＶＰＮサービス条件テーブル１４に該当するＶＰＮサービス条件が存在するか否か確認し、また、該当する値が許容値内であるか否かを判定する。

11

【００６９】ＶＰＮサービス条件設定手段２４は、カスタマ識別子およびＶＰＮ識別子に基づき、個々のＶＰＮサービス条件項目に対して、ＶＰＮサービスオーダに含まれる値を現在の値として設定する。

【００７０】次に図９を参照すると、ＶＰＮサービスエージェント３は、カスタマからＶＰＮサービス条件を変更するオーダが発生したとき、当該カスタマ網５に付与されている現ＶＰＮサービス条件を、ＶＰＮサービス条件テーブル（図７）から検索するＶＰＮサービス条件検索手段３１と、上記の検索したＶＰＮサービス条件に基づいて、上記のオーダをＶＰＮサービスマネージャ２に対して発行するＶＰＮサービスオーダ発行手段３２と、を備えている。

【００７１】またＶＰＮサービスエージェント３は、ＶＰＮサービスマネージャ２が、ＶＰＮサービスエージェント３経由でカスタマエッジＣＥを制御するとき、上記のオーダを受けてＶＰＮサービスマネージャ２により設定し直されたＶＰＮサービス条件に基づきカスタマエッジＣＥを制御するカスタマエッジ制御手段３３を備える。

【００７２】なお、Ｃ－ＮＭＳ１３には、Ｃ－ｉｐ網（図６）の障害監視およびトラヒック監視等、といったＶＰＮサービス条件の変更（ＶＰＮサービスオーダ）を発行するためのＩＰ網情報を収集する機能群が配置されている。

【００７３】さらに説明を補足すると、ＶＰＮサービスオーダ発行手段３２は、Ｃ－ＮＭＳ１３から得られるＩＰ網情報を元に、個々のＶＰＮサービス条件に対して値を変更するオーダを、ＶＰＮサービスマネージャ３に対して発行する。

【００７４】カスタマエッジ制御手段３３は、カスタマエッジＣＥが実装しているＶＰＮサービスに関する機能の制御を行う手段である。

【００７５】以上図７、図８および図９によって説明したことをベースにして、再び図６に戻り、既述のイベントＥ１，Ｅ２，Ｅ３…を、制御シーケンスの形で説明する。

【００７６】図１０は図６での制御シーケンスを説明するためのフローチャート（その１）、図１１は同フローチャート（その２）、である。

【００７７】まずこれら図１０および図１１の各ステップ（Ｓ１１～Ｓ１９）と、図６の各イベント（Ｅ１～Ｅ５）とを対応づけると、

Ｅ１：Ｓ１１，Ｓ１２およびＳ１３

Ｅ２：Ｓ１４

Ｅ３：Ｓ１５，Ｓ１６およびＳ１７

Ｅ４：Ｓ１８

Ｅ５：Ｓ１９

のようになる。ステップＳ１１～Ｓ１９は次のとおりである。

12

【００７８】ステップＳ１１：Ｃ－ｉｐ網のＶＰＮサービス管理者は、Ｃ－ＮＭＳ１３のＣ－ｉｐ網情報および所定の網運行予定からＶＰＮサービス条件変更を判断する。

【００７９】ステップＳ１２：ＶＰＮサービスエージェント３のＶＰＮサービス条件検索手段３１は当該カスタマのＶＰＮサービス条件を取得する。

【００８０】ステップＳ１３：Ｃ－ｉｐ網のＶＰＮサービス管理者が、ＶＰＮサービスオーダを、ＶＰＮサービスエージェント３に発行する。

【００８１】ステップＳ１４：ＶＰＮサービスエージェント３のＶＰＮサービスオーダ発行手段３２は、ＶＰＮサービスオーダをＶＰＮサービスマネージャ２に送信する。

【００８２】ステップＳ１５：ＶＰＮサービスマネージャ２のＶＰＮサービスオーダ制御手段２１は、ＶＰＮサービスオーダをＶＰＮサービス条件判定手段２３に発行する。

【００８３】ステップＳ１６：上記の判定の結果が、「可」（ＯＫ）か「不可」（ＮＧ）か判定する。

【００８４】ステップＳ１７：ＶＰＮサービスマネージャ２のＣＥ制御手段２５は、ＶＰＮサービスオーダに基づくＣＥ制御を実行する。

【００８５】ステップＳ１８：ＶＰＮサービスマネージャ２は、ＶＰＮサービスエージェント３にＶＰＮサービスオーダの結果を応答する。

【００８６】ステップＳ１９：ＶＰＮサービスマネージャ２は、隣接するＶＰＮサービスエージェント３にＶＰＮサービスオーダの結果を通知する。

【００８７】以上の構成（図７、図８、図９）および制御シーケンス（図１０、図１１）により、カスタマ側ＩＰ網のＶＰＮサービス運用者は、任意かつ動的に、プロバイダ側ＩＰ網のＶＰＮサービス運用者を介することなく、ＶＰＮサービス条件を変更することが可能となる。このことは、ＶＰＮサービスカスタマ側のＶＰＮサービス運用者が、仮想的なカスタマＩＰ網全体の利用状況や予測に基づき、かつ、タイムリーにカスタマＩＰ網の効率的運用を可能とすることを意味する。

【００８８】図１２は本発明の適用事例を示す図であり、図１３は図１２の適用事例で用いるＶＰＮサービス条件テーブル１４の内容を示す図である。

【００８９】なお、図１２の見方は前述の図６とほぼ同じであり、図１３は図７に示すＶＰＮサービス条件テーブル１４の詳細例である。該テーブル１４は図１２のデータベース（ＤＢ）１５内に形成される。

【００９０】図１２および図１３を参照しながら、本発明の適用事例を説明する。

【００９１】あるカスタマである、Ｗｅｂチケット販売サービスを行っている企業ｃｉが、単一のカスタマ網管理システムＣ－ＮＭＳ１３により監視制御される２つの

13

カスタマＩＰ網ｃｉｐ１およびｃｉｐ２を有し、プロバイダＩＰ網Ｐ－ｉｐにより、ｃｉｐ１とｃｉｐ２との間で、ＶＰＮサービスが提供されている。

【００９２】このとき、カスタマエッジはＣＥ１およびＣＥ２、プロバイダエッジはＰＥ１およびＰＥ２であり、提供されているＶＰＮは、ＣＥ１からＰＥ１およびＰＥ２を経てＣＥ２に至るＶＰＮｃｉである。また、ＶＰＮサービス条件テーブル１４を格納するデータベース（ＤＢ）１５は、Ｐ－ＮＭＳ１２内に設置されている例を示す。

【００９３】この企業ｃｉに提供されているＶＰＮｃｉに対するＶＰＮサービス条件としては、ＶＰＮサービスの帯域幅を任意に変更できるものとし、その帯域の現在の値、最大値、最小値および設定幅は、図１３に示すとおりそれぞれｂｗ－ｉ，ｂｗ－ｍａｘ，ｂｗ－ｍｉｎおよびｂｗΔである（ｂｗ：ｂａｎｄｗｉｄｔｈ）。この場合の企業ｃｉのカスタマ識別子およびＶＰＮ識別子はそれぞれｃｉ－ｉｄおよびＶＰＮｃｉ－ｉｄであり、ＶＰＮｃｉの両端点（Ａ，Ｚ）であるＣＥ１およびＣＥ２のＣＥ識別子はそれぞれＣＥ１－ｉｄおよびＣＥ２－ｉｄである。

【００９４】なおＶＰＮサービスを実現するためには以上に述べた以外にも、ＣＥ１とＰＥ１間、ＰＥ１とＰＥ２間、ＰＥ２とＣＥ２間のＶＰＮリンクや、ＶＰＮを実現するための、より下位のネットワーク技術が存在する。

【００９５】ここで、チケット販売期間中に、チケット購入希望者からのオーダが殺到するためにＶＰＮｃｉ（つまりｃｉｐ１，ｃｉｐ２間）のアクセス量が急増する。このためにＶＰＮサービス条件を迅速に変更することになる。この場合の制御は以下のようになる。

【００９６】１．ＶＰＮｃｉのＶＰＮサービス管理者は、チケット販売開始時にＶＰＮサービス帯域（帯域幅）の変更が必要であると判断する。

【００９７】２．ＶＰＮサービス管理者は、ＶＰＮサービスエージェント（ＶＰＮａ）３のＶＰＮサービス条件検索手段３１により、ＤＢ１５からＶＰＮｃｉのＶＰＮサービス条件（ＶＰＮサービス帯域）を取得し、帯域幅ｂｗをｂｗ’だけ増加することを決定する。

【００９８】３．ＶＰＮサービス管理者は、カスタマ識別子ｃｉとＶＰＮ識別子ＶＰＮｃｉ－ｉｄとに対応するＶＰＮサービス帯域を、ｂｗからｂｗ’に変更するオーダ（ｏｒｄｅｒ）をサービスエージェント（ＶＰＮａ）３に対して発行する。

【００９９】４．そのサービスエージェントＶＰＮａのＶＰＮサービスオーダ発行手段３２は、そのオーダをＶＰＮサービスマネージャ（ＶＰＮｍ）２に送信する。

【０１００】５．このサービスマネージャＶＰＮｍのＶＰＮサービスオーダ制御手段２１は、当該オーダをＶＰＮサービス条件判定手段２３に対して発行する。

14

【０１０１】６．このＶＰＮサービス条件判定手段２３は、そのオーダに含まれる変更帯域ｂｗ’が、データベース１５内のｂｗ－ｍａｘおよびｂｗ－ｍｉｎに対し下記の条件を満足するか否か評価する。

【０１０２】ｂｗ－ｍｉｎ＜ｂｗ’＜ｂｗ－ｍａｘ

上記条件を満足するならば、ＶＰＮサービス条件判定手段２３はそのオーダについて、判定結果「ＯＫ」を返すが、上記条件を満足しないならば判定結果「ＮＧ」を返すことになる（図７のステップＳ１６）。

【０１０３】７．ＶＰＮサービスオーダ制御手段２１は、ＶＰＮサービス条件判定手段２３から受取る判定結果が「ＯＫ」である場合、ＶＰＮサービス条件設定手段２４に対して当該オーダを発行するが、ＶＰＮサービス条件判定手段２３から受取る判定結果が「ＮＧ」である場合には、上記エージェントＶＰＮａに対してオーダ失敗の応答を行って本制御は終了する。

【０１０４】８．ＶＰＮサービス条件設定手段２４は、ＶＰＮｃｉに付与されたサービス条件であるＶＰＮサービス帯域の現在の値を、ｂｗからｂｗ’に変更する。

【０１０５】９．さらにＶＰＮサービスオーダ制御手段２１は、上記７．での判定結果が「ＯＫ」である場合には、ＣＥ１およびＣＥ２に対して、ｂｗをｂｗ’とする制御をＣＥ制御手段２５により実行する。

【０１０６】１０．ＶＰＮサービスオーダ制御手段２１はまた上記９．での、ＣＥ１とＣＥ２に対する制御結果を、エージェントＶＰＮａに対する応答として返す。

【０１０７】１１．チケット販売の終了時には、ＶＰＮサービス帯域を再度ｂｗ’から元のｂｗに変更すべく、上記２．～１０．について、オーダがｂｗとなる制御を実施することになる。

【０１０８】以上により、企業によるｃｉチケット販売期間中は、ＶＰＮｃｉのＶＰＮサービス帯域を増加させることで、チケット購入希望者のアクセス殺到に対応できることになる。

【０１０９】さらに補足的に図１に示すシステムの具体的イメージを図を用いて示す。

【０１１０】図１４は図１に示すＶＰＮサービス管理システムの具体的イメージを示す図（その１）であり、図１５は同図（その２）である。

【０１１１】図１４において、右側（プロバイダ側）および左側（カスタマ側）には、それぞれＶＰＮサービス管理システム１の、ＶＰＮサービスマネージャ２およびＶＰＮサービスエージェント３が示されている。

【０１１２】ＶＰＮサービスマネージャ２の主たる機能として、ＶＰＮサービスオーダ制御機能（図８の手段２１参照）が示されている。この機能を果すための本来的な動作として、該ＶＰＮサービスマネージャ２は、図示するポリシー（Ｐｏｌｉｃｙ）制御、ＱｏＳ（Ｑｕａｌｉｔｙ　ｏｆ　Ｓｅｒｖｉｃｅ）管理、在庫管理等を行っている。在庫管理とは、例えばあるカスタマが現在１

０Ｍｂｐｓの帯域で運用中のところ、急に１００Ｍｂｐｓへ帯域を増大したいとの要求をそのカスタマから受けたときに、その増大要求を受け入れられるか否かを判断するための、いわゆるリソース管理を行うことを意味する。

【０１１３】またそのＶＰＮサービスマネージャ２と協働するプロバイダ網管理システム（Ｐ－ＮＭＳ）１２は、図示する障害（ａ）、構成（ｂ）、性能（ｃ）および機密（ｄ）の各管理部を少なくとも有する。ＶＰＮサービスマネージャ２は、これらの管理部ａ～ｄによる管理データに基づいて、同システム（Ｐ－ＮＭＳ）１２内のＯＳをもとに、ＮＥ（Ｎｅｔｗｏｒｋ　Ｅｌｅｍｅｎｔ）通信制御部２６ならびに該当するポート（Ｐｏｒｔ）を介して、配下のプロバイダ網４内のＰＥ，ＣＥ，ＰＣＲ等の各機器（ＮＥ）を制御する。

【０１１４】上記障害管理部ａは、プロバイダ網４内に発生した各種の障害を常に把握している。

【０１１５】上記構成管理部ｂは、プロバイダ網４がどのような機器（ＮＥ）によって構成されているかを常に把握している。

【０１１６】上記性能管理部ｃは、上記各機器におけるトラヒック情報やパケットロスの発生量等を常に監視している。

【０１１７】また上記機密管理部ｄは、パスワードや認証による照合チェックを行う。

【０１１８】他方、図１４の左側（カスタマ側）に設けられるＶＰＮサービスエージェント３の主たる機能として、カスタマエッジ（ＣＥ）トラヒック監視機能、ＶＰＮサービス品質要求制御機能およびカスタマＶＰＮ障害監視機能が示されており、ＯＳをもとに、該当のポート（Ｐｏｒｔ）を介して、カスタマエッジＣＥの監視を行う。

【０１１９】図１４に示すＶＰＮサービス管理システム１における処理は以下の（１）、（２）および（３）に大別される。なお（１）、（２）および（３）は図１４の中にも示されている。

【０１２０】（１）例えば、図３のカスタマＡ網－１，２，３および４を通じて、当該カスタマＡである企業の社長がその企業の全拠点の従業員に対して一斉に経営方針についての放映が行われるような場合、当該ＶＰＮサービスエージェント３はＶＰＮサービスマネージャ２に対し、「カスタマＶＰＮサービス条件の変更を要求」する。つまり帯域幅（ｂｗ）の一時的な増大を求める。

【０１２１】（２）その要求を受けたＶＰＮサービスマネージャ２は、配下のプロバイダ網管理システム（Ｐ－ＮＭＳ）１２に対し、「ＶＰＮサービス条件の変更を要求」する。

【０１２２】（３）その要求を受けたプロバイダ網管理システム１２は、配下のプロバイダ網４内の各機器（ＮＥ）に対し、「ＶＰＮサービス条件の変更をすべき旨のコマンド」を送出する。

【０１２３】次に図１５を参照する。本図は、図１４の構成においてさらに実際のイメージを表したものである。

【０１２４】この図１５においては、ＶＰＮサービスエージェント３の中に、ＶＰＮサービスオーダ発行機能（図９の手段３２参照）とＶＰＮサービス条件検索機能（図９の手段３１参照）が示されている。

【０１２５】本図の左上に示すｅは、ＶＰＮサービス品質要求メニューである。このメニューｅは、ＶＰＮサービスマネージャ２から提示された、マネージャ２より提供可能な各種サービスのリストに対して、カスタマ側から提供を求めるサービスを特定してマネージャ２に返すメニューである。

【０１２６】さらにｇは、カスタマ側においてカスタマエッジＣＥにおけるトラヒックの時間推移を調べるためのＣＥトラヒックビューである。このトラヒックビューｇを参照することによって、当該カスタマ側の運用管理者は、現在の使用帯域の状況を知ることができる。

【０１２７】またｆは、カスタマのＶＰＮを可視的にトポロジーとして運用管理者に見せるためのビューである。このビューｆは実際には、ＶＰＮの障害監視のために利用するためのＶＰＮ障害監視ビューである。

【０１２８】〔第２の態様〕次に、本発明に係るＶＰＮサービス管理システム１における、ＶＰＮサービス管理の完全自動化について説明する。

【０１２９】図１６は本発明に係る第２の態様（完全自動化）を説明するためのＶＰＮサービス管理システム１を示す図である。

【０１３０】ただし本図の大半は前述の図５と同じである。異なるのは、カスタマ管理センター８内に、カスタマ網管理センター（Ｃ－ＮＭＳ）１３が明示されたことである。これは、Ｃ－ＮＭＳ１３とＰ－ＮＭＳ１２との連携によって上記の完全自動化が達成されることを表すためである。

【０１３１】第２の態様のポイントは次のような構成にある。すなわち、カスタマ網管理システム（Ｃ－ＮＭＳ１３）がカスタマ網５の運用状況を監視しその監視結果に応じて、ＶＰＮサービスエージェント３と、ＶＰＮサービスマネージャ２およびプロバイダ網管理システム（Ｐ－ＮＭＳ）１２と、の連携により、ＶＰＮサービス条件の変更をオペレータの介在なしに完全自動で行う、という構成である。

【０１３２】さらに具体的には、ＶＰＮサービスエージェント３は、ＶＰＮサービス条件を変更する際に参照すべき変更条件データを予め設定して保持するパラメータテーブルを有し、カスタマ網管理システム１３は、上記の監視結果によって、ＶＰＮサービス条件を変更すべきであると判断したとき、上記のパラメータテーブルを参照して決定された変更ＶＰＮサービス条件を、ＶＰＮサ

ービスマネージャに送信するように構成する。

【０１３３】図１７は図１６に示すＶＰＮサービス管理システム１の具体的イメージを示す図である。

【０１３４】本図の大半は前述の図１４と同じである。異なるのは、上述したパラメータテーブルが参照番号３４として示されており、また、該パラメータテーブル３４を参照するＶＰＮサービス変更判定部３５が示されていることである。動作は大別して図中の（１）、（２）、（３）および（４）で示される。

【０１３５】（１）Ｃ－ＮＭＳ１３はまずカスタマ網５のトラヒックとサービス品質のデータを収集する。

【０１３６】（２）Ｃ－ＮＭＳ１３は他方、パラメータテーブル３４を参照して、当該カスタマに付与されているＶＰＮサービス条件を検索する。

【０１３７】（３）上記（１）において収集した上記データを、パラメータテーブル３４内に格納された域値と比較し、そのデータが域値を超えたことを検出すると、域値超えの警告をＶＰＮサービス変更判定部３５に通知する。これはサービスオーダの発行機能（図９の手段３２）である。

【０１３８】（４）上記ＶＰＮサービス変更判定部３５は上記の通知を受けると、パラメータテーブル３４を参照して、上記域値超えをカバーし得るＶＰＮサービス品質への変更を求める要求を、オペレータの介在なしに自動的に、ＶＰＮサービスマネージャ２に伝える。

【０１３９】かくしてＶＰＮサービスマネージャ２は、その要求に見合うように、プロバイダ網４内の機器（ＮＥ）の制御を行う。

【０１４０】以上を具体的に要約すると、カスタマ網５へのインターネット等のアクセス頻度、カスタマエッジＣＥへのトラヒック流量等カスタマ網５の運用状態に関する条件を、Ｃ－ＮＭＳ１３が管理する。ＶＰＮサービスエージェント３は、これらの条件がある域値を超えた場合の、その域値種別や増分度合い等と、ＶＰＮサービスパラメータ変更条件とを、ＶＰＮパラメータとしてパラメータテーブル３４に保持する。

【０１４１】Ｃ－ＮＭＳ１３が、カスタマ網５の運用条件の域値を超えたことを検出した場合、ＶＰＮサービスエージェント３は、パラメータテーブル３４を参照した後、その参照した変更条件を、ＶＰＮサービスマネージャ２とＰ－ＮＭＳ１２とにより、プロバイダ網４に反映することにより、カスタマ網５の運用状態に応じたＶＰＮサービス条件を、カスタマ網５の運用管理者やプロバイダ網４の運用管理者の介在なしに、即座に満足させることができる。ここで上記パラメータテーブルについて簡単に説明しておく。

【０１４２】図１８はパラメータテーブル３４を図解的に示す図である。

【０１４３】本図の上段のテーブルの内容は、前述した図７の上段に示すテーブル１４の内容と同じである。本図の上段のテーブル３４の内容に対し、ＶＰＮサービス変更判定部３５は、本図の下段に一例を示すような変更の判定を行う。その判定のレベルは、複数のレベルからなる。

【０１４４】レベル１は、現状値がＢｅｓｔ　Ｅｆｆｏｒｔ型の値をとるものとすると、その値から２０％ｕｐに変更する。

【０１４５】レベル２は、現状値が上記２０％ｕｐの値だとすると、その５０％ｕｐに変更する。

【０１４６】レベル３は、現状値が上記５０％ｕｐの値だとすると、その１００％ｕｐに変更する。つまりレベルが上がる程、変更帯域幅が増大する。

【０１４７】次に上述した第２の態様のもとでの動作を説明する。

【０１４８】図１９は図１６に示す第２の態様のもとでの一連のシーケンスを示す図である。

【０１４９】今仮に、ＶＰＮサービスの提供を受けている企業が、ある時間帯に突然ネットワークの輻輳状態になったものとする。このため、その企業はＶＰＮサービス条件を急に変更することを望む。この変更は、下記の手順で自動的に行われる。

【０１５０】（１）カスタマ側のＣ－ＮＭＳ１３が域値超えを判断すると、ＶＰＮサービスエージェント３はトラヒック域値超えアラームを通知する（図中の（１））。

【０１５１】ＶＰＮサービス変更判定部３５は、Ｃ－ＮＭＳの域値超えを判断する。その判断ロジックは、該判定部３５内に予め組み込まれている。その内容は例えば以下のとおりである。

【０１５２】

【表１】

レベル	パケットロス	トラヒックスレショルド
レベル1	障害メッセージ1個	スレショルド90%，5回
レベル2	障害メッセージ5個	スレショルド90%，10回
⋮	⋮	⋮

【０１５３】（２）ＶＰＮサービスエージェント３は、パラメータテーブル３４を参照する（図中の（２））。そしてパラメータをもとに現在のサービスと比較し、ＶＰＮサービス条件の最適レベルを選択する。

【０１５４】（３）新たなＶＰＮサービス条件が選択されると、ＶＰＮサービスエージェント３は新たなＶＰＮサ

ービスへの変更要求を、自動的に、ＶＰＮサービスマネージャ２に要求する（図中の（３））。

【０１５５】（４）上記要求の通知を受けたＶＰＮサービスマネージャ２は、現状の該カスタマの使用帯域を読み取り、その変更の要求の可否を判断する（図中の（４））。

【０１５６】変更不可であれば、ＶＰＮサービスマネージャ２より、「不可」の旨を該カスタマのＶＰＮサービスエージェント３に通知する。

【０１５７】（５）逆に変更要求が「可」であれば、そのサービス変更を、機器設定変更コマンドとして、Ｐ－ＮＭＳ１２に通知する（図中の（５））。

【０１５８】（６）Ｐ－ＮＭＳ１２は、パラメータテーブル３４に示す条件に従って、プロバイダ側のＮＥに対し、例えばポリシー設定等の機器設定変更コマンドを発行する。これによって企業側のＶＰＮサービス内容が変更される。この例によれば、ネットワークの帯域幅が広くなって、輻輳を解消し、また、パケットロスを抑制することが、自動的に実現される（図中の（６））。

【０１５９】（７）ＮＥの設定変更に成功すると、Ｐ－ＮＭＳ１２にその成功を通知する（図中の（７））。

【０１６０】（８）以上による新たなサービスへの変更に成功すると、Ｐ－ＮＭＳ１２はその旨の返答をＶＰＮサービスマネージャ２に対して行う（図中の（８））。

【０１６１】（９）ＶＰＮサービスマネージャ２は、当該ＶＰＮサービスを利用してカスタマ側のＶＰＮサービスエージェント３に通知する（図中の（９））。

【０１６２】（１０）ＶＰＮサービスエージェント３は新たなサービスへの変更が通知されると、データベース（パラメータテーブル３４を格納するデータベース）に現サービスのパラメータを記録する（図中の（１０））。

【０１６３】以上のように、ある期間中のＶＰＮサービス帯域を増大させることにより、ネットワークの輻輳への対応が自動的に行えることになる。

【０１６４】〔第３の態様〕次に、本発明に係るＶＰＮサービス管理システムにおける、ＶＰＮサービス管理の半自動化について説明する。

【０１６５】図２０は本発明に係る第３の態様（半自動化）を説明するためのＶＰＮサービス管理システム１を示す図である。

【０１６６】ただし本図の大半は前述の図１６と同じである。異なるのは、カスタマ管理センター８内に置かれたクライアント端末４１および遠隔地の遠隔クライアント端末４２が示されていること、および運用状態変更通知手段４３が示されていることである。なお、上記クライアント端末４１および４２を総称して運用管理者（４０）とも称す。

【０１６７】第３の態様のポイントは次のような構成にある。すなわち、カスタマ網管理システム（Ｃ－ＮＭＳ）１３がカスタマ網５の運用状況を監視しその監視結果によって、ＶＰＮサービス条件を変更すべきであると判断したとき、その判断をカスタマ網５の運用管理者４０に通知する運用状態変更通知手段４３を前記ＶＰＮサービスエージェント３に設け、このＶＰＮサービスエージェント３は、上記の通知に対する許可応答を得たとき、ＶＰＮサービスマネージャ２およびプロバイダ網管理システム（Ｐ－ＮＭＳ）１２との連携により、ＶＰＮサービス条件の変更を半自動で行う、という構成である。

【０１６８】さらに具体的には、ＶＰＮサービスエージェント３は、ＶＰＮサービス条件を変更する際に参照すべき変更条件データを予め設定して保持するパラメータテーブル３４（図１７参照）を有し、カスタマ網管理システム（Ｃ－ＮＭＳ）１３が、上記の監視結果によって、ＶＰＮサービス条件を変更すべきであると判断したとき、そのパラメータテーブル３４を参照して決定された変更ＶＰＮサービス条件を、運用状態変更通知手段４３に入力するように構成する。

【０１６９】なお、本第３の態様に基づくＶＰＮサービス管理システム１の具体的イメージを示す図は、前述の図１７とほぼ同様であるので省略するが、該システム１の具体的イメージを要約すると次のとおりである。

【０１７０】ＶＰＮサービスエージェント３は、既述した域値種別や増分度合い等と、ＶＰＮサービスパラメータ変更条件とを、ＶＰＮパラメータテーブル３４（図１８参照）と共に、カスタマ網５の運用管理者４０へ通知する運用状態変更通知手段４３を有する。

【０１７１】Ｃ－ＮＭＳ１３が、カスタマ網５の運用条件の域値を超えたことを検出した場合、ＶＰＮサービスエージェント３は、パラメータテーブル３４を参照した後、運用管理者４０にその事実を通知する。そして、運用管理者４０の判断を、ＶＰＮサービスマネージャ２とＰ－ＮＭＳ１２とにより、プロバイダ網４に反映させる。これにより、カスタマ網５の運用状態に応じたＶＰＮサービス条件を、運用管理者４０の判断の元で、プロバイダ網４のオペレータの介在なしに、即座に、満足させることができる。

【０１７２】図２１は図２０に示す第３の態様のもとでの一連のシーケンスを示す図である。

【０１７３】本図は前述の図１９のシーケンス図と近似しており、相互に同様のプロセスには同一の番号を（　）を付して示す。

【０１７４】今仮に、ＶＰＮサービスの提供を受けている企業が、ある時間帯に突然ネットワークの輻輳になったものとすると、下記のプロセス（１）、（２）、…が次の順に進行する。なお、（１１）、（１２）等は本第３の態様に固有のプロセスである。

【０１７５】（１）図１９の（１）に同じ。

【０１７６】（２）図１９の（２）に同じ。

【０１７７】（１１）ＶＰＮサービスエージェント３によって選択されたサービスレベル（図１８の下段参照）が、運用管理者４０に通知される（図中の（１１））。

【０１７８】（１２）運用管理者４０は、この新たなサービスレベルを当該企業に適用するか否か判断し、その結果を、ＶＰＮサービスエージェント３に返答する（図中の（１２））。

【０１７９】（３）上記変更要求についての判断結果を通知されたＶＰＮサービスエージェント３は、その結果を新たなＶＰＮサービス変更要求として、自動的にＶＰＮサービスマネージャ２に要求する。

【０１８０】（４）～（９）は、図１９の（４）～（９）に同じ。

【０１８１】（１３）以上によりＶＰＮサービス条件の設定が変更されたので、これをＣ－ＮＭＳ１３に反映させる。半自動化の場合は、前述の完全自動化の場合と異なり、最終的な結果をＣ－ＮＭＳ１３が確認できないので、このプロセス（１３）が必要である。

【０１８２】以上のように、ある期間中のＶＰＮサービス帯域を増大させることにより、ネットワークの輻輳への対応が、半自動で、行えることになる。

【０１８３】以上述べたように、半自動化ＶＰＮサービスでは、予め設定されたパラメータテーブル３４は、域値を超えるか、または、超える予測通知があった場合、パラメータテーブル３４のサービス条件を参照し、ＶＰＮサービス変更判定部３５（図１７参照）によって、どのようなサービスを選択すべきかを自動的に判断する。このときその判断を、前記通知手段４３に入力する。当該入力に基づき、運用管理者４０（オペレータ）は、サービス変更判定部３５による判断結果を最終的に再確認し、サービス内容の変更に問題がない場合には、上記オペレータはプロバイダ網４のＶＰＮサービスマネージャ２に対して、サービス内容の変更を要求する。

【０１８４】かくしてカスタマ網５の運用状態に応じたＶＰＮサービス条件を、プロバイダ網４の運用管理者の介在なしに、即座に満足させることができる。

【０１８５】〔第４の態様〕次に、本発明に係るＶＰＮサービス管理システム１における、サーバ／クライアント型の管理について説明する。

【０１８６】図２２は本発明に係る第４の態様（サーバ／クライアント型）を説明するためのＶＰＮサービス管理システム１を示す図である。

【０１８７】ただし本図の大半は前述の図２０と同じである。異なるのは、運用状態変更通知手段４３が、サーバ／クライアント形態で実現されていることである。

【０１８８】第４の態様のポイントは次のような構成にある。すなわち、ＶＰＮサービスエージェント３とカスタマ網管理システム（Ｐ－ＮＭＳ）１３とが、サーバ／クライアント形態で連携するとき、当該クライアントの他の１つとして、運用管理者４０に付帯する遠隔クライアント端末４２を導入し、ＶＰＮサービスエージェント３と遠隔クライアント端末４２とを、サーバ／クライアント形態で連携させることにより、運用状態変更通知手段４３を実現する、という構成である。

【０１８９】さらに好ましくは、ＶＰＮサービスエージェント３と遠隔クライアント端末４２とが、専用線またはイン－バンドで接続されるようにする。

【０１９０】図２３は図２２に示すＶＰＮサービス管理システム１の具体的イメージを示す図である。

【０１９１】本図の大半は前述の図１７と同じである。異なるのは、上述した運用状態変更通知手段４３が、ＶＰＮサービス変更通知部４４として示されていることである。また、動作を表わす（１）、（２）、（３）および（４）のうち、動作（３）が異なる。第４の態様では、この（３）において、ＶＰＮサービス変更通知部４４がＶＰＮサービスパラメータ変更の通知をＣ－ＮＭＳ１３側から受け取る。

【０１９２】図２２および図２３の構成を要約すると、運用状態変更通知手段４３を、Ｃ－ＮＭＳ１３やＶＰＮサービスエージェント３が稼動するオペレーション端末（４１，４２）上への警告表示手段として、実現することができる。カスタマ網管理センター８以外の場所に端末があり、遠隔クライアント端末４２として、ＶＰＮサービスエージェント３に接続している。

【０１９３】遠隔操作の場合、運用管理者端末（４１，４２）と、ＶＰＮサービスエージェント３とは、サーバおよびクライアントの関係になり、相互に社内ＬＡＮまたはイン－バンド（ｉｎ－ｂａｎｄ）にて接続される。

【０１９４】図２４は図２２に示す第４の態様のもとでの一連のシーケンスを示す図である。

【０１９５】本図は図２１のシーケンス図とほぼ同じであり、同様のプロセスには同一の番号を（ ）を付して示す。特に異なるのは、図２４の上段において、ＶＰＮサービスエージェント３と運用管理者４０の端末（４１，４２）とが、サーバ／クライアントとして表されていることである。

【０１９６】したがって、本図のプロセス（１）～（１３）は、図２１のプロセス（１）～（１３）と同じであるが、遠隔操作によるＶＰＮサービスという点で、上記第３の態様とは異なる。

【０１９７】このＶＰＮサービスは、カスタマ網５の運用責任者（社長、オペレータ等）は随時遠隔クライアント４２によって、プロバイダ側にサービス変更要求を依頼することができる。遠隔クライアント４２は、カスタマ網５のサービスエージェント３と接続しており、カスタマ網４の運用責任者の判断によって、前記パラメータテーブル３４上のサービス条件を決定する。その結果に基づき、サービスエージェント３側からプロバイダ網４のＶＰＮサービスマネージャ２に対して、サービス内容を要求する。遠隔クライアント４２は、カスタマ網５の

サービスエージェント３は、専用線またはインーバンド（ｉｎ－ｂａｎｄ）にて接続されているため、セキュリティ上の問題はない。

【０１９８】また、上記の遠隔操作によって、運用管理者４０は固定した場所だけではなく、離れた場所でもＶＰＮの管理を行うことができる。以上のように、ある期間中のＶＰＮサービス帯域を増大させることにより、ネットワークの輻輳への対応が、遠隔操作で、行えることになる。

【０１９９】〔第５の態様〕次に、本発明に係るＶＰＮサービス管理システム１における、遠隔許可応答型の管理について説明する。

【０２００】図２５は本発明に係る第５の態様（遠隔許可応答型）を説明するためのＶＰＮサービス管理システム１を示す図である。

【０２０１】ただし本図の大半は前述の図１６と同じである。異なるのは、一例として、ＲＡＮ（Ｒａｄｉｏ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）５１とモバイル端末５２とが示されていることである。

【０２０２】第５の態様のポイントは次のような構成にある。すなわち、カスタマ網管理システム（Ｃ－ＮＭＳ）１３がカスタマ網５の運用状況を監視しその監視結果に応じて、自動的にＶＰＮサービスマネージャ２に対しＶＰＮサービス条件の変更を要求したとき、その要求を受けて、カスタマである遠隔の運用管理者４０に確認を求める運用状態変更確認手段５３をＶＰＮサービスマネージャ２側に設け、ＶＰＮサービスマネジャー２は、上記の通知に対する許可応答を得たとき、ＶＰＮサービス条件の変更を行う、という構成である。

【０２０３】さらに具体的には、上記の運用状態変更確認手段５３は、前記ＶＰＮサービスマネージャ２と、前記プロバイダ網に無線で接続されるモバイル端末５２と、で実現する。

【０２０４】この場合、前述したように、ＶＰＮサービスエージェント３は、ＶＰＮサービス条件を変更する際に参照すべき変更条件データを予め設定して保持するパラメータテーブル３４を有し、カスタマ網管理システム１３は、前述の監視結果によって、前述のＶＰＮサービス条件を変更すべきであると判断したとき、そのパラメータテーブル３４を参照して決定された変更ＶＰＮサービス条件を、ＶＰＮサービスマネージャ２に送信する。

【０２０５】図２６は図２５に示す第５の態様のもとでの一連のシーケンスを示す図である。

【０２０６】本図は図２１のシーケンス図と近似しており、同様のプロセスには同一の番号を（　）を付して示す。特に異なるのは、図２６の上段において、モバイル端末４２と運用状態変更確認手段５３が表わされていることである。また、プロセスについて見ると、図２１の通知プロセス（１１）は、図２６において、ＶＰＮサービスマネージャ２に伸びる通知プロセス（２１）となり、運用管理者（モバイル端末５２）に、プロセス（２１）を介しての変更要求の確認をするプロセス（２２）が追加され、その確認により得た許可応答を、モバイル端末５２からマネージャ２に返すプロセス（２３）が追加される。

【０２０７】図２５および図２６の構成を要約すると、ＶＰＮサービスにおいて、運用状態変更確認手段５３として、インターネットメールや携帯電話（５２）により、カスタマ網５の運用管理センター８以外の場所からも、ＶＰＮサービス条件の変更を行えるようにしたものである。つまり、カスタマ網管理センター８以外のモバイル端末５２があり、遠隔操作により半自動でＶＰＮサービス制御を行う。

【０２０８】モバイル端末５２（カスタマ運用管理者）への情報の通知は、プロバイダ網４のＲＡＮ５１を介して行われる。なお、上記のような態様の確認が行われることの、カスタマ運用管理者（５２）への連絡の方法は次のとおりである。

【０２０９】図２７は運用管理者への連絡方法を図解的に表す図であり、図２８は運用管理者との間での事前準備について図解的に表す図である。

【０２１０】図２７によれば、予め運用管理者４０の端末４１にて、上記の連絡方法（連絡手段）を選択する。

【０２１１】次に連絡先のメールアドレス（Ｍａｉｌ）または携帯電話の番号（Ｍｏｂｉｌｅ）を入力する。

【０２１２】図２８を参照すると、モバイル端末５２に通知するメールの内容が例示されている。

【０２１３】上記の事前準備として、ＶＰＮサービス条件の契約内容を設定しておく必要があり、その内容の一例を図２８に示す。

【０２１４】モバイル端末４２で制御を行うに当り、モバイル端末４２での操作をシンプルにするため、上記の事前準備として、契約内容を予め設定する。また端末５２の所有者の返答も簡単に行えるようにする。例えば、＃キーを押して番号を入力する。端末５２への通知は音声またはメール形式でよい。

【０２１５】かくして運用管理者４０は、メールアドレスまたはモバイル端末の番号の選択によって、ダイナミックにＶＰＮサービス条件を変更可能となり、カスタマ網５の管理者が不在のときでも、カスタマのＶＰＮサービスに影響を及ぼすことがない。

【０２１６】つまり、カスタマ側の運用管理者４０は網管理センター８にいなくても、ＶＰＮサービス帯域を増大させる等、のＶＰＮサービス条件の設定が可能である。

【０２１７】〔第６の態様〕次に、本発明に係るＶＰＮサービス管理システム１における、マネージャーエジェント間の通信形態について説明する。

【０２１８】図２９は第６の態様を適用した図１７の構成を示す図である。

【０２１９】したがって本図の大半は図１７の構成と同じである。異なるのは、カスタマ側のインーバンド手段６１と、プロバイダ側のインーバンド手段６２とが表されていることである。

【０２２０】第６の態様のポイントは次のような構成にある。すなわち、ＶＰＮサービスマネージャ２とＶＰＮサービスエージェント３との間の連携のために、プロバイダとカスタマとの間の契約により構築したＶＰＮそれ自身をインーバンドに使用するインーバンド手段を有する、という構成である。

【０２２１】具体的には、そのインーバンド手段６１および６２は、カスタマエッジＣＥと、プロバイダ網４内にカスタマエッジＣＥとの接続用に配備されるプロバイダエッジＰＥとに、それぞれ、図示の６１および６２として、形成される。

【０２２２】このようにインーバンドを利用することから、図１７における（４）の動作（「ＶＰＮサービス条件変更オーダ」）は、図２９に示す、インーバンドによる経路６３にて行われる。

【０２２３】要約すれば第６の態様によれば、ＶＰＮサービスエージェント３とＶＰＮサービスマネージャ２との間の通信手段として、プロバイダとカスタマとの間で契約したＶＰＮ自身を、インーバンドに使用することで、新たな独立な通信手段を導入することなしに、ＶＰＮサービス条件の変更に関する通信を行うことができる。また同時にセキュリティの確保も行える。

【０２２４】次に、上記インーバンドについて説明する。

【０２２５】図３０は本発明に係るインーバンド手段について説明するための図である。

【０２２６】本図において、カスタマエッジＣＥには、監視用ポートでの情報を、ＶＰＮインーバンドに転送するための仕組み（インーバンド手段６１）を備える。

【０２２７】同様に、プロバイダエッジＰＥには、監視用ポートでの情報を、ＶＰＮインーバンドに転送するための仕組み（インーバンド手段６２）を備える。

【０２２８】このプロバイダエッジに必要な仕組みを実現するためには、次の２つの情報（ｉ）および（ii）を、プロバイダエッジＰＥ上の所要データ（ｃｏｎｆｉｇｕｒａｔｉｏｎ　ｄａｔａ）として、事前に設定する。

【０２２９】（ｉ）当該プロバイダエッジＰＥを管理するＶＰＮサービスエージェント３のＩＰアドレス。

【０２３０】（ii）カスタマとプロバイダとの間で経由すべきＶＰＮの識別子（ＶＰＮ－ｉｄ）。

【０２３１】一方、上記カスタマエッジＣＥに必要な仕組みを実現するためには、ＣＥとＶＰＮサービスエージェント３との接続方法を考えなければならない。この接続方法についてその２案を図に示す。

【０２３２】図３１はＣＥとエージェント３との間の第１の接続方法を表す図であり、図３２はＣＥとエージェント３との間の第２の接続方法を表す図である。

【０２３３】図３１は、ネットワークを介さずに直接ＣＥ側の保守端末用イーサネット（登録商標）・ポート（ｐｏｒｔ）からエージェント３に接続する方法を示す。

【０２３４】図３２は、ネットワーク（カスタマ網５）を介して、ＣＥとエージェント３を接続する方法を示す。

【０２３５】図３３はマネージャ２とエージェント３との間のインーバンドによる接続例を示す図である。

【０２３６】本図に従って説明する。

【０２３７】（１）前記の（ii）すなわちＶＰＮ－ｉｄによって、当該ＶＰＮ（カスタマＡ網）のＣＥまで制御情報が到達する。その後、（２）前記の２つの接続方法（図３１、図３２）のいずれかによって、ネットワーク（カスタマＡ網）側へ制御情報が出て行き、（３）前記の（ｉ）すなわちＩＰアドレスにより、目的のＩＰアドレスのＶＰＮサービスエージェントＡ（３－Ａ）まで、制御情報が到着する、ことができる。

【０２３８】なお、ＰＥとＶＰＮサービスマネージャ２間の通信手段については、独立のＶＰＮ網を設定する方法や、ＰＥからその途中まで、既存ＶＰＮを間借りし、その途中とＶＰＮサービスマネージャ２との間はＩＰネットワークを利用する方法等、既知の技術がある。

【０２３９】以上本発明に係るＶＰＮサービス管理システム１の全体について詳述した。しかし本発明はそのシステム１の全体にのみ特徴があるのではなく、そのシステム１を構成する、ＶＰＮサービスマネージャ２自体とＶＰＮサービスエージェント３自体とにも特徴がある。これらのＶＰＮサービスマネージャ２自体の特徴的な構成と、ＶＰＮサービスエージェント３自体の特徴的な構成とを、前述した図１～図３０に基づく説明をもとにまとめてみる。

【０２４０】まず、ＶＰＮサービスマネージャ２自体についてその特徴的な構成は、以下のとおりである。

【０２４１】（Ａ）ＶＰＮサービスマネージャ２は、カスタマを収容するカスタマ網５と、該カスタマにＶＰＮサービスを提供するプロバイダによって構築されカスタマ網５に連結するプロバイダ網４と、を備える通信網に対しＶＰＮサービスの管理を行うためのＶＰＮサービス管理システム１を構成するＶＰＮサービスマネージャである。

【０２４２】このマネージャ２は、プロバイダ網４に対してＶＰＮサービスの管理を行うと共に、カスタマ網５に対してＶＰＮサービスの管理を行うＶＰＮサービスエージェント３と連携して、ＶＰＮサービスエージェント３の管理下にあるカスタマ網５の運用状況に応じて、ＶＰＮサービス管理システム１が提供すべきＶＰＮサービスのＶＰＮサービス条件をリアルタイムに変更するよう

に構成する。

【０２４３】さらにこのマネージャ２は、ＶＰＮサービスエージェント３からＶＰＮサービス条件を変更するオーダが発生したときこれを受信して、該オーダに係る変更ＶＰＮサービス条件を出力するＶＰＮサービスオーダ制御手段２１と、そのオーダが発生したとき、当該カスタマ網５に付与されている現ＶＰＮサービス条件を、ＶＰＮサービス条件テーブル１４から検索するＶＰＮサービス条件検索手段２２と、上記の変更ＶＰＮサービス条件が現ＶＰＮサービス条件から超える範囲が許容範囲か否か判定するＶＰＮサービス条件判定手段２３と、上記の判定の結果が「可」であるとき、現ＶＰＮサービス条件をその変更ＶＰＮサービス条件に設定し直すＶＰＮサービス条件設定手段２４と、上記の設定し直されたＶＰＮサービス条件に基づきカスタマエッジＣＥを制御するカスタマエッジ制御手段２５と、を備えて構成される。

【０２４４】ここにマネージャ２は、カスタマ網管理システム（Ｃ－ＮＭＳ）１３がカスタマ網５の運用状況を監視しその監視結果に応じて、自動的に、ＶＰＮサービス条件の変更がカスタマ網管理システム１３から要求されたとき、その要求をカスタマ網５の運用管理者４０に通知する運用状態変更通知手段４３を有し、上記の通知に対する許可応答を得たとき、ＶＰＮサービス条件の変更を行うように構成する。

【０２４５】（Ｂ）一方、ＶＰＮサービスエージェント３は、カスタマを収容するカスタマ網５と、該カスタマにＶＰＮサービスを提供するプロバイダによって構築されカスタマ網５に連結するプロバイダ網４と、を備える通信網に対しＶＰＮサービスの管理を行うためのＶＰＮサービス管理システム１を構成するＶＰＮサービスエージェントである。

【０２４６】このエージェント３は、カスタマ網５に対してＶＰＮサービスの管理を行うと共に、プロバイダ網４に対してＶＰＮサービスの管理を行うＶＰＮサービスマネージャ３と連携して、管理下にあるカスタマ網５の運用状況に応じて、ＶＰＮサービス管理システム１が提供すべきＶＰＮサービスのＶＰＮサービス条件をリアルタイムに変更するように構成される。

【０２４７】さらにこのエージェント３は、カスタマ網５を管理するカスタマ網管理システム（Ｃ－ＮＭＳ）１３を有し、このカスタマ網管理システム１３は、カスタマエッジＣＥを監視しかつプロバイダ網４側との通信を行うように構成する。

【０２４８】そしてこのエージェント３は、ＶＰＮサービスに関するサービスメニューを、ＶＰＮサービス条件テーブル１４としてＶＰＮサービスマネージャ２より提供され、カスタマ側にてＶＰＮサービス条件の変更要求が発生したとき、その変更要求を上記サービスメニューを介してＶＰＮサービスマネージャ２に送信するように構成される。

【０２４９】またこのエージェント３は、カスタマからＶＰＮサービス条件を変更するオーダが発生したとき、当該カスタマ網５に付与されている現ＶＰＮサービス条件を、ＶＰＮサービス条件テーブル１４から検索するＶＰＮサービス条件検索手段３１と、上記の検索したＶＰＮサービス条件に基づいて、オーダをＶＰＮサービスマネージャ２に対して発行するＶＰＮサービスオーダ発行手段３２と、を備えるように構成される。

【０２５０】さらにこのエージェント３は、ＶＰＮサービス条件を変更する際に参照すべき変更条件データを予め設定して保持するパラメータテーブル３４を有し、カスタマ網管理システム（Ｃ－ＮＭＳ）１３は、上記の監視結果によって、ＶＰＮサービス条件を変更すべきであると判断したとき、そのパラメータテーブル３４を参照して決定された変更ＶＰＮサービス条件を、ＶＰＮサービスマネージャ２に送信するように構成する。

【０２５１】さらにまた、このエージェント３は、カスタマ網管理システム１３がカスタマ網５の運用状況を監視しその監視結果によって、ＶＰＮサービス条件を変更すべきであると判断したとき、その判断をカスタマ網５の運用管理者４０に通知する運用状態変更通知手段４３を有し、上記の通知に対する許可応答を得たとき、ＶＰＮサービスマネージャ２およびプロバイダ網管理システム（Ｐ－ＭＮＳ）１２との連携により、ＶＰＮサービス条件の変更を行うように構成する。

【０２５２】以上詳述した本発明の実施態様は以下のとおりである。

【０２５３】（付記１）　カスタマを収容するカスタマ網と、該カスタマにＶＰＮサービスを提供するプロバイダによって構築され該カスタマ網に連結するプロバイダ網と、を備える通信網に対し該ＶＰＮサービスの管理を行うためのＶＰＮサービス管理システムであって、前記プロバイダ網に対して前記ＶＰＮサービスの管理を行うＶＰＮサービスマネージャと、前記カスタマ網に対して前記ＶＰＮサービスの管理を行うＶＰＮサービスエージェントと、を有し、前記ＶＰＮサービスマネージャは前記ＶＰＮサービスエージェントと連携し、該ＶＰＮサービスエージェントの管理下にある前記カスタマ網の運用状況に応じて、提供すべき前記ＶＰＮサービスのＶＰＮサービス条件をリアルタイムに変更することを特徴とするＶＰＮサービス管理システム。

【０２５４】（付記２）　前記プロバイダ側に前記ＶＰＮサービスマネージャと協働するプロバイダ網管理システムをさらに有し、該プロバイダ網管理システムは、前記カスタマ網内に前記プロバイダ網との接続用に配備されるカスタマエッジをも含めて該プロバイダ網を管理することを特徴とする付記１に記載のＶＰＮサービス管理システム。

【０２５５】（付記３）　前記カスタマ側に前記ＶＰＮサービスエージェントと協働すると共に前記カスタマ網

を管理するカスタマ網管理システムをさらに有し、該カスタマ網管理システムは、前記カスタマエッジを監視しかつ前記プロバイダ網側との通信を行うことを特徴とする付記２に記載のＶＰＮサービス管理システム。

【０２５６】（付記４）　前記ＶＰＮサービスマネージャは、ＶＰＮサービスに関するサービスメニューをＶＰＮサービス条件テーブルとして前記ＶＰＮサービスエージェントに提供し、前記カスタマ側にてＶＰＮサービス条件の変更要求が発生したとき、該ＶＰＮサービスエージェントは前記サービスメニューを介してその変更要求を該ＶＰＮサービスマネージャに送信し、該ＶＰＮサービスマネージャは、前記プロバイダ網管理システムを介して、その変更要求を前記プロバイダ網に反映させることを特徴とする付記２に記載のＶＰＮサービス管理システム。

【０２５７】（付記５）　前記ＶＰＮサービスマネージャは、前記ＶＰＮサービスエージェントから前記ＶＰＮサービス条件を変更するオーダが発生したときこれを受信して、該オーダに係る変更ＶＰＮサービス条件を出力するＶＰＮサービスオーダ制御手段と、前記オーダが発生したとき、当該カスタマ網に付与されている現ＶＰＮサービス条件を、ＶＰＮサービス条件テーブルから検索するＶＰＮサービス条件検索手段と、前記変更ＶＰＮサービス条件が前記現ＶＰＮサービス条件から超える範囲が許容範囲か否か判定するＶＰＮサービス条件判定手段と、前記の判定の結果が「可」であるとき、前記現ＶＰＮサービス条件を前記変更ＶＰＮサービス条件に設定し直すＶＰＮサービス条件設定手段と、前記の設定し直されたＶＰＮサービス条件に基づきカスタマエッジを制御するカスタマエッジ制御手段と、を備えることを特徴とする付記１に記載のＶＰＮサービス管理システム。

【０２５８】（付記６）　前記ＶＰＮサービスエージェントは、前記カスタマから前記ＶＰＮサービス条件を変更するオーダが発生したとき、当該カスタマ網に付与されている現ＶＰＮサービス条件を、ＶＰＮサービス条件テーブルから検索するＶＰＮサービス条件検索手段と、前記の検索したＶＰＮサービス条件に基づいて、前記オーダを前記ＶＰＮサービスマネージャに対して発行するＶＰＮサービスオーダ発行手段と、を備えることを特徴とする付記１に記載のＶＰＮサービス管理システム。

【０２５９】（付記７）　前記ＶＰＮサービスマネージャが、前記ＶＰＮサービスエージェント経由でカスタマエッジを制御するとき、前記オーダを受けて該ＶＰＮサービスマネージャにより設定し直されたＶＰＮサービス条件に基づきカスタマエッジを制御するカスタマエッジ制御手段を備えることを特徴とする付記６に記載のＶＰＮサービス管理システム。

【０２６０】（付記８）　前記カスタマ網管理システムが前記カスタマ網の運用状況を監視しその監視結果に応じて、前記ＶＰＮサービスエージェントと、前記ＶＰＮサービスマネージャおよび前記プロバイダ網管理システムと、の連携により、前記ＶＰＮサービス条件の変更をオペレータの介在なしに完全自動で行うことを特徴とする付記３に記載のＶＰＮサービス管理システム。

【０２６１】（付記９）　前記ＶＰＮサービスエージェントは、前記ＶＰＮサービス条件を変更する際に参照すべき変更条件データを予め設定して保持するパラメータテーブルを有し、前記カスタマ網管理システムは、前記監視結果によって、前記ＶＰＮサービス条件を変更すべきであると判断したとき、前記パラメータテーブルを参照して決定された変更ＶＰＮサービス条件を、前記ＶＰＮサービスマネージャに送信することを特徴とする付記８に記載のＶＰＮサービス管理システム。

【０２６２】（付記１０）　前記カスタマ網管理システムが前記カスタマ網の運用状況を監視しその監視結果によって、前記ＶＰＮサービス条件を変更すべきであると判断したとき、その判断を前記カスタマ網の運用管理者に通知する運用状態変更通知手段を前記ＶＰＮサービスエージェントに設け、該ＶＰＮサービスエージェントは、前記の通知に対する許可応答を得たとき、前記ＶＰＮサービスマネージャおよび前記プロバイダ網管理システムとの連携により、前記ＶＰＮサービス条件の変更を半自動で行うことを特徴とする付記３に記載のＶＰＮサービス管理システム。

【０２６３】（付記１１）　前記ＶＰＮサービスエージェントは、前記ＶＰＮサービス条件を変更する際に参照すべき変更条件データを予め設定して保持するパラメータテーブルを有し、前記カスタマ網管理システムが、前記監視結果によって、前記ＶＰＮサービス条件を変更すべきであると判断したとき、前記パラメータテーブルを参照して決定された変更ＶＰＮサービス条件を、前記運用状態変更通知手段に入力することを特徴とする付記１０に記載のＶＰＮサービス管理システム。

【０２６４】（付記１２）　前記ＶＰＮサービスエージェントと前記カスタマ網管理システムとが、サーバ／クライアント形態で連携するとき、該クライアントの他の１つとして、前記運用管理者に付帯する遠隔クライアント端末を導入し、前記ＶＰＮサービスエージェントと前記遠隔クライアント端末とを、サーバ／クライアント形態で連携させることにより、前記運用状態変更通知手段を実現することを特徴とする付記１０に記載のＶＰＮサービス管理システム。

【０２６５】（付記１３）　前記ＶＰＮサービスエージェントと前記遠隔クライアント端末とが、専用線またはインーバンドで接続されることを特徴とする付記１２に記載のＶＰＮサービス管理システム。

【０２６６】（付記１４）　前記カスタマ網管理システムが前記カスタマ網の運用状況を監視しその監視結果に応じて、自動的に前記ＶＰＮサービスマネージャに対し前記ＶＰＮサービス条件の変更を要求したとき、その要

求を受けて、前記カスタマである遠隔の運用管理者に確認を求める運用状態変更確認手段を前記ＶＰＮサービスマネージャ側に設け、該ＶＰＮサービスマネジャーは、前記の通知に対する許可応答を得たとき、前記ＶＰＮサービス条件の変更を行うことを特徴とする付記３に記載のＶＰＮサービス管理システム。

【０２６７】（付記１５）　前記運用状態変更確認手段は、前記ＶＰＮサービスマネージャと、前記プロバイダ網に無線で接続されるモバイル端末と、で実現することを特徴とする付記１４に記載のＶＰＮサービス管理システム。

【０２６８】（付記１６）　前記ＶＰＮサービスエージェントは、前記ＶＰＮサービス条件を変更する際に参照すべき変更条件データを予め設定して保持するパラメータテーブルを有し、前記カスタマ網管理システムは、前記監視結果によって、前記ＶＰＮサービス条件を変更すべきであると判断したとき、前記パラメータテーブルを参照して決定された変更ＶＰＮサービス条件を、前記ＶＰＮサービスマネージャに送信することを特徴とする付記１４に記載のＶＰＮサービス管理システム。

【０２６９】（付記１７）　前記ＶＰＮサービスマネージャと前記ＶＰＮサービスエージェントとの間の前記の連携のために、前記プロバイダと前記カスタマとの間の契約により構築したＶＰＮそれ自身をインーバンドに使用するインーバンド手段を有することを特徴とする付記３に記載のＶＰＮサービス管理システム。

【０２７０】（付記１８）　前記インーバンド手段は、前記カスタマエッジと、前記プロバイダ網内に該カスタマエッジとの接続用に配備されるプロバイダエッジとに、それぞれ形成されることを特徴とする付記３に記載のＶＰＮサービス管理システム。

【０２７１】（付記１９）　カスタマを収容するカスタマ網と、該カスタマにＶＰＮサービスを提供するプロバイダによって構築され該カスタマ網に連結するプロバイダ網と、を備える通信網に対し該ＶＰＮサービスの管理を行うためのＶＰＮサービス管理システムを構成するＶＰＮサービスマネージャであって、前記プロバイダ網に対して前記ＶＰＮサービスの管理を行うと共に、前記カスタマ網に対して前記ＶＰＮサービスの管理を行うＶＰＮサービスエージェントと連携して、該ＶＰＮサービスエージェントの管理下にある前記カスタマ網の運用状況に応じて、前記ＶＰＮサービス管理システムが提供すべき前記ＶＰＮサービスのＶＰＮサービス条件をリアルタイムに変更することを特徴とするＶＰＮサービスマネージャ。

【０２７２】（付記２０）　前記ＶＰＮサービスエージェントから前記ＶＰＮサービス条件を変更するオーダが発生したときこれを受信して、該オーダに係る変更ＶＰＮサービス条件を出力するＶＰＮサービスオーダ制御手段と、前記オーダが発生したとき、当該カスタマ網に付

与されている現ＶＰＮサービス条件を、ＶＰＮサービス条件テーブルから検索するＶＰＮサービス条件検索手段と、前記変更ＶＰＮサービス条件が前記現ＶＰＮサービス条件から超える範囲が許容範囲か否か判定するＶＰＮサービス条件判定手段と、前記の判定の結果が「可」であるとき、前記現ＶＰＮサービス条件を前記変更ＶＰＮサービス条件に設定し直すＶＰＮサービス条件設定手段と、前記の設定し直されたＶＰＮサービス条件に基づきカスタマエッジを制御するカスタマエッジ制御手段と、を備えることを特徴とする付記１９に記載のＶＰＮサービスマネージャ。

【０２７３】（付記２１）　前記カスタマ網管理システムが前記カスタマ網の運用状況を監視しその監視結果に応じて、自動的に、前記ＶＰＮサービス条件の変更が該カスタマ網管理システムから要求されたとき、その要求を前記カスタマ網の運用管理者に通知する運用状態変更通知手段を有し、前記の通知に対する許可応答を得たとき、前記ＶＰＮサービス条件の変更を行うことを特徴とする付記１９に記載のＶＰＮサービスマネージャ。

【０２７４】（付記２２）　カスタマを収容するカスタマ網と、該カスタマにＶＰＮサービスを提供するプロバイダによって構築され該カスタマ網に連結するプロバイダ網と、を備える通信網に対し該ＶＰＮサービスの管理を行うためのＶＰＮサービス管理システムを構成するＶＰＮサービスエージェントであって、前記カスタマ網に対して前記ＶＰＮサービスの管理を行うと共に、前記プロバイダ網に対して前記ＶＰＮサービスの管理を行うＶＰＮサービスマネージャと連携して、管理下にある前記カスタマ網の運用状況に応じて、前記ＶＰＮサービス管理システムが提供すべき前記ＶＰＮサービスのＶＰＮサービス条件をリアルタイムに変更することを特徴とするＶＰＮサービスエージェント。

【０２７５】（付記２３）　前記カスタマ網を管理するカスタマ網管理システムをさらに有し、該カスタマ網管理システムは、前記カスタマエッジを監視しかつ前記プロバイダ網側との通信を行うことを特徴とする付記２２に記載のＶＰＮサービスエージェント。

【０２７６】（付記２４）　ＶＰＮサービスに関するサービスメニューを、ＶＰＮサービス条件テーブルとして前記ＶＰＮサービスマネージャより提供され、前記カスタマ側にてＶＰＮサービス条件の変更要求が発生したとき、その変更要求を前記サービスメニューを介して該ＶＰＮサービスマネージャに送信することを特徴とする付記２２に記載のＶＰＮサービスエージェント。

【０２７７】（付記２５）　前記カスタマから前記ＶＰＮサービス条件を変更するオーダが発生したとき、当該カスタマ網に付与されている現ＶＰＮサービス条件を、ＶＰＮサービス条件テーブルから検索するＶＰＮサービス条件検索手段と、前記の検索したＶＰＮサービス条件に基づいて、前記オーダを前記ＶＰＮサービスマネージ

ャに対して発行するＶＰＮサービスオーダ発行手段と、を備えることを特徴とする付記２２に記載のＶＰＮサービスエージェント。

【０２７８】（付記２６）　前記ＶＰＮサービス条件を変更する際に参照すべき変更条件データを予め設定して保持するパラメータテーブルを有し、前記カスタマ網管理システムは、前記監視結果によって、前記ＶＰＮサービス条件を変更すべきであると判断したとき、前記パラメータテーブルを参照して決定された変更ＶＰＮサービス条件を、前記ＶＰＮサービスマネージャに送信することを特徴とする付記２３に記載のＶＰＮサービスエージェント。

【０２７９】（付記２７）　前記カスタマ網管理システムが前記カスタマ網の運用状況を監視しその監視結果によって、前記ＶＰＮサービス条件を変更すべきであると判断したとき、その判断を前記カスタマ網の運用管理者に通知する運用状態変更通知手段をさらに有し、前記の通知に対する許可応答を得たとき、前記ＶＰＮサービスマネージャおよび前記プロバイダ網管理システムとの連携により、前記ＶＰＮサービス条件の変更を行うことを特徴とする付記２３に記載のＶＰＮサービスエージェント。

【０２８０】

【発明の効果】以上詳述したように本発明によれば、ＶＰＮサービスにおいて、下記の効果を得ることができる。

【０２８１】１）カスタマとプロバイダとの間での契約条件を変更したいというカスタマ側の要求に対し、迅速に応えることができる。

【０２８２】２）ＩＰ－ＶＰＮサービス等のＶＰＮサービスの品質条件や利用条件を簡単に変更することができる。

【０２８３】３）カスタマとプロバイダとの間での契約によって締結した、サービス品質の合意を常に遵守することができる。ＩＰ－ＶＰＮサービス等のＶＰＮサービス管理システムを実現することを目的とするものである。

【図面の簡単な説明】

【図１】本発明に係るＶＰＮサービス管理システムの基本構成図である。

【図２】従来の典型的なＶＰＮサービスネットワークを図解的に示す図である。

【図３】本発明により形成されるＶＰＮサービスネットワークを図解的に示す図である。

【図４】本発明に係るＶＰＮサービス管理システムの全体を表す図である。

【図５】本発明に係るＶＰＮサービス管理システム１の基本構成を示す図である。

【図６】図５の構成を具体例によって示す図である。

【図７】ＶＰＮサービス条件テーブルを図解的に表す図である。

【図８】ＶＰＮサービスマネージャ２が有する機能を表す図である。

【図９】ＶＰＮサービスエージェント３が有する機能を表す図である。

【図１０】図６での制御シーケンスを説明するためのフローチャート（その１）である。

【図１１】図６での制御シーケンスを説明するためのフローチャート（その２）である。

【図１２】本発明の適用事例を示す図である。

【図１３】図１２の適用事例で用いるＶＰＮサービス条件テーブル１４の内容を示す図である。

【図１４】図１に示すＶＰＮサービス管理システムの具体的イメージを示す図（その１）である。

【図１５】図１に示すＶＰＮサービス管理システムの具体的イメージを示す図（その２）である。

【図１６】本発明に係る第２の態様（完全自動化）を説明するためのＶＰＮサービス管理システム１を示す図である。

【図１７】図１６に示すＶＰＮサービス管理システム１の具体的イメージを示す図である。

【図１８】パラメータテーブル３４を図解的に示す図である。

【図１９】図１６に示す第２の態様のもとでの一連のシーケンスを示す図である。

【図２０】本発明に係る第３の態様（半自動化）を説明するためのＶＰＮサービス管理システム１を示す図である。

【図２１】図２０に示す第３の態様のもとでの一連のシーケンスを示す図である。

【図２２】本発明に係る第４の態様（サーバ／クライアント型）を説明するためのＶＰＮサービス管理システム１を示す図である。

【図２３】図２２に示すＶＰＮサービス管理システム１の具体的イメージを示す図である。

【図２４】図２２に示す第４の態様のもとでの一連のシーケンスを示す図である。

【図２５】本発明に係る第５の態様（遠隔許可応答型）を説明するためのＶＰＮサービス管理システム１を示す図である。

【図２６】図２５に示す第５の態様のもとでの一連のシーケンスを示す図である。

【図２７】運用管理者への連絡方法を図解的に表す図である。

【図２８】運用管理者との間での事前準備について図解的に表す図である。

【図２９】第６の態様を適用した図１７の構成を示す図である。

【図３０】本発明に係るインーバンド手段について説明するための図である。

35

【図３１】ＣＥとエージェント３との間の第１の接続方法を表す図である。

【図３２】ＣＥとエージェント３との間の第２の接続方法を表す図である。

【図３３】マネージャ２とエージェント３との間のインーバンドによる接続例を示す図である。

【符号の説明】

１…ＶＰＮサービス管理システム
２…ＶＰＮサービスマネージャ（プロバイダ側）
３…ＶＰＮサービスエージェント（カスタマ側）
４…プロバイダ網
５…カスタマ網
６…キャリア網
７…プロバイダ網管理センター
８…カスタマ網管理センター
１２…プロバイダ網管理システム（Ｐ－ＮＭＳ）
１３…カスタマ網管理システム（Ｃ－ＮＭＳ）
１４…ＶＰＮサービス条件テーブル
１５…データベース（ＤＢ）
２１…ＶＰＮサービスオーダ制御手段
２２…ＶＰＮサービス条件検索手段
２３…ＶＰＮサービス条件判定手段
２４…ＶＰＮサービス条件設定手段

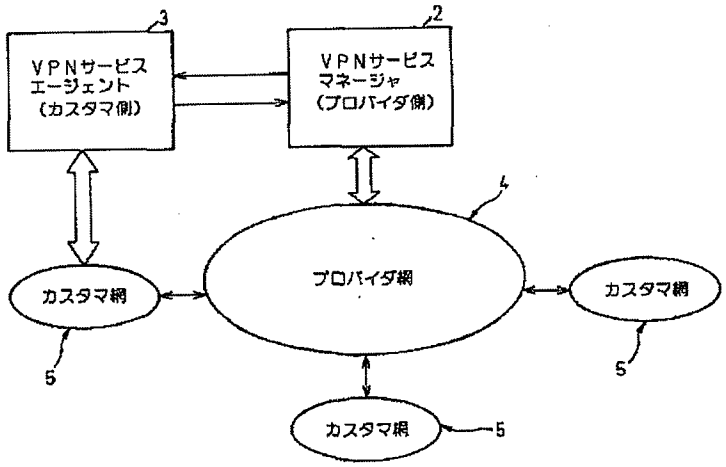
36

２５…カスタマエッジ制御手段
２６…ＮＥ通信制御部
３１…ＶＰＮサービス条件検索手段
３２…ＶＰＮサービスオーダ発行手段
３３…カスタマエッジ制御手段
３４…パラメータテーブル
３５…ＶＰＮサービス変更判定部
４０…運用管理者
４１…クライアント端末
４２…遠隔クライアント端末
４３…運用状態変更通知手段
４４…ＶＰＮサービス変更通知部
５１…ＲＡＮ
５２…モバイル端末
５３…運用状態変更確認手段
６１…インーバンド手段（カスタマ側）
６２…インーバンド手段（プロバイダ側）
６３…インーバンドによる経路
ＣＥ…カスタマエッジ
ＰＥ…プロバイダエッジ
ＣＲ…カスタマルータ
ＰＣＲ…プロバイダコアルータ

【図１】

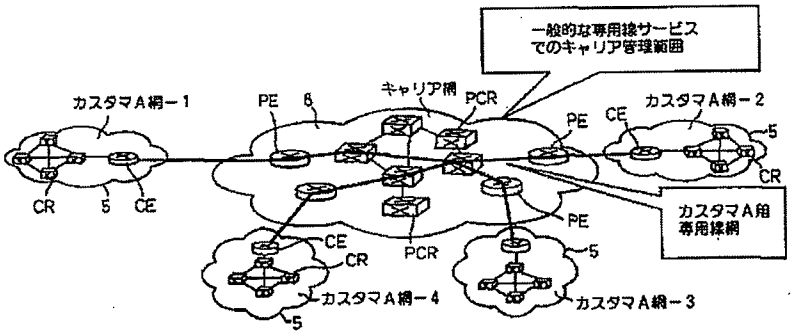
本発明に係るＶＰＮサービス管理システムの基本構成図

図１



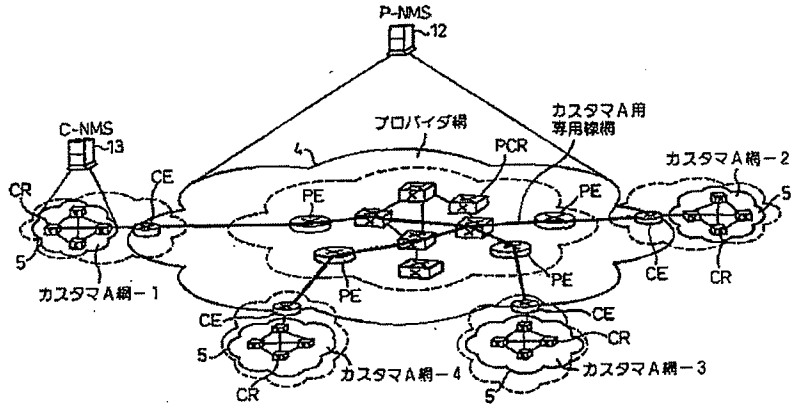
【図２】

従来の典型的なＶＰＮサービスネットワークを図解的に示す図　図２



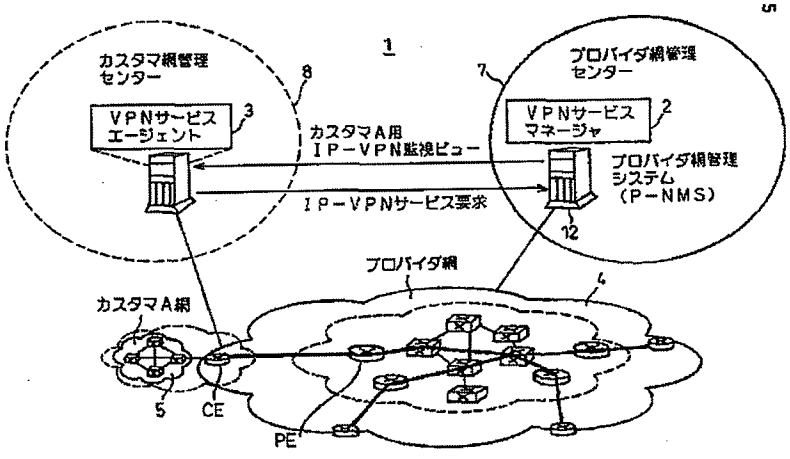
【図３】

本発明により形成されるＶＰＮサービスネットワークを図解的に示す図　図３



【図５】

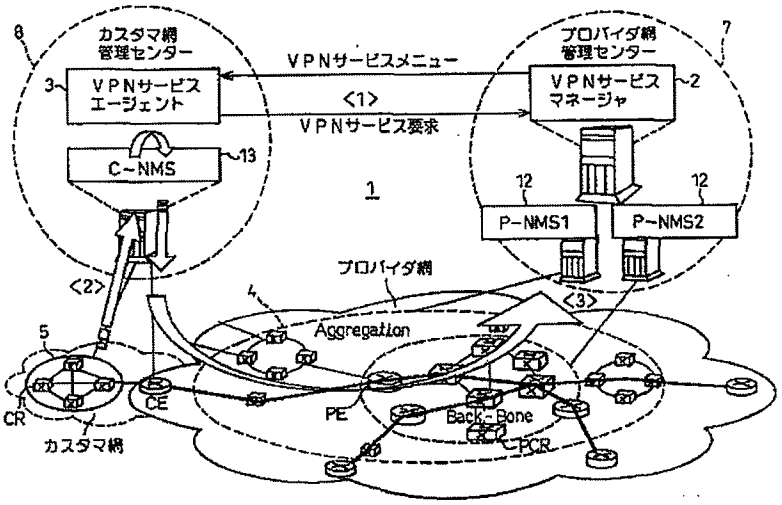
本発明に係るＶＰＮサービス管理システム１の基本構成を示す図　図５



【図４】

図４

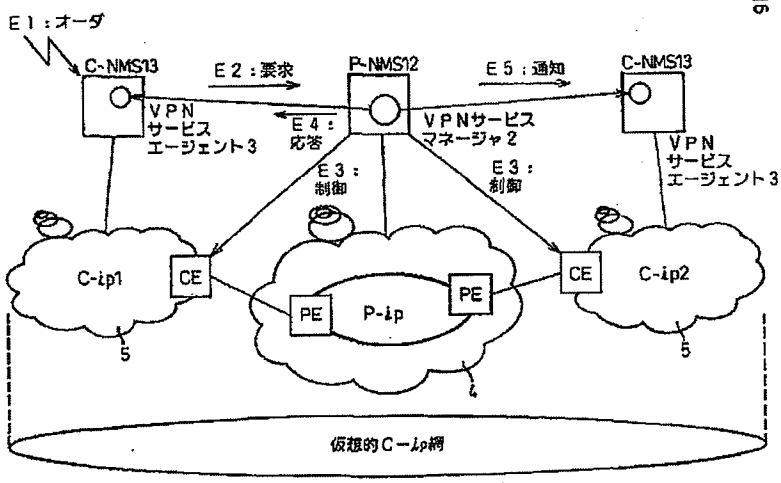
本発明に係るＶＰＮサービス管理システムの全体を表す図



【図６】

図６

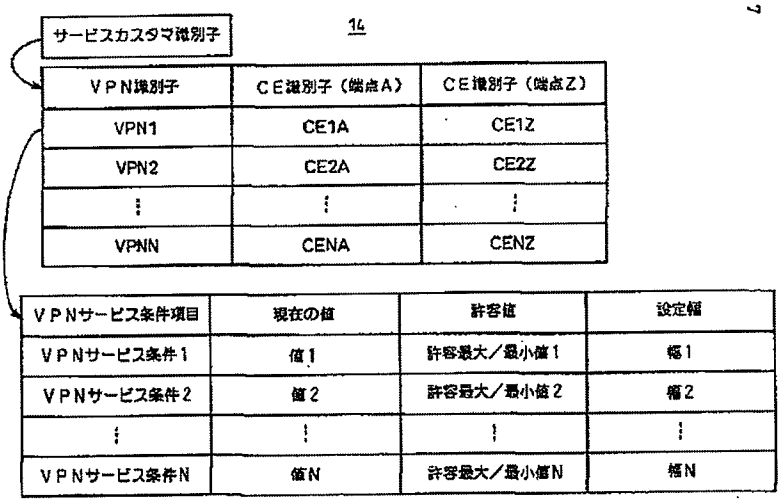
図５の構成を具体例によって示す図



【図７】

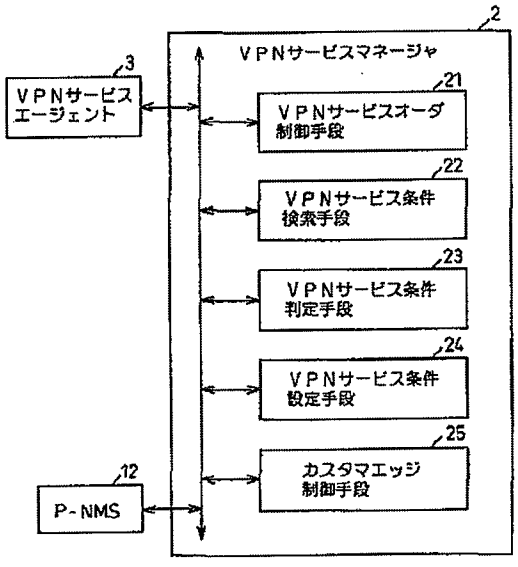
図７

ＶＰＮサービス条件テーブルを図解的に表す図



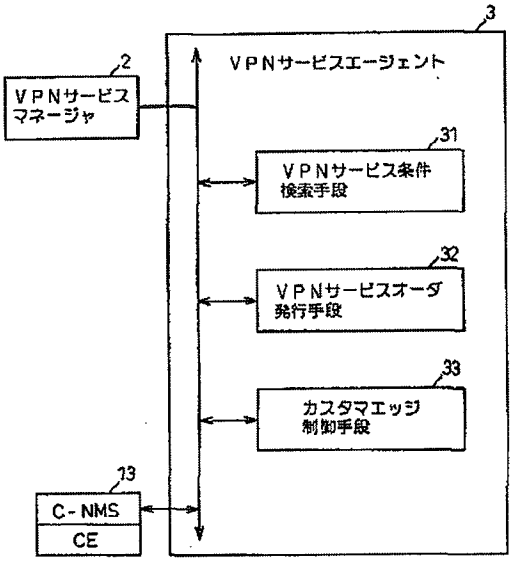
【図８】

図８　ＶＰＮサービスマネージャ２が有する機能を表す図



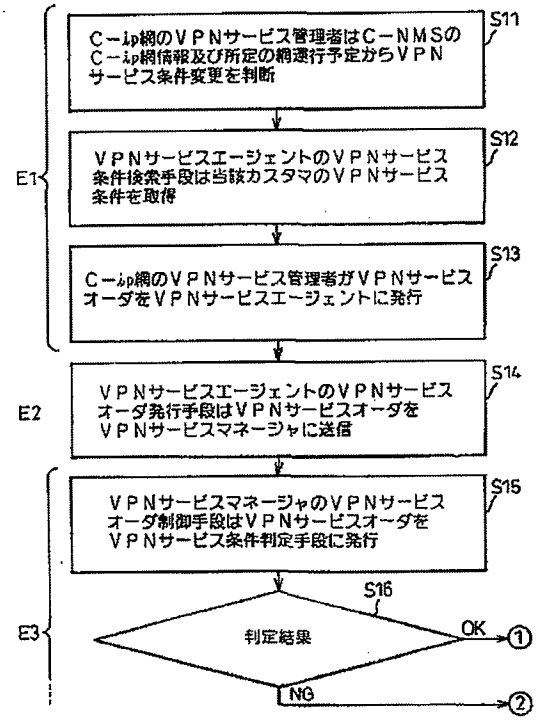
【図９】

図９　ＶＰＮサービスエージェント３が有する機能を表す図



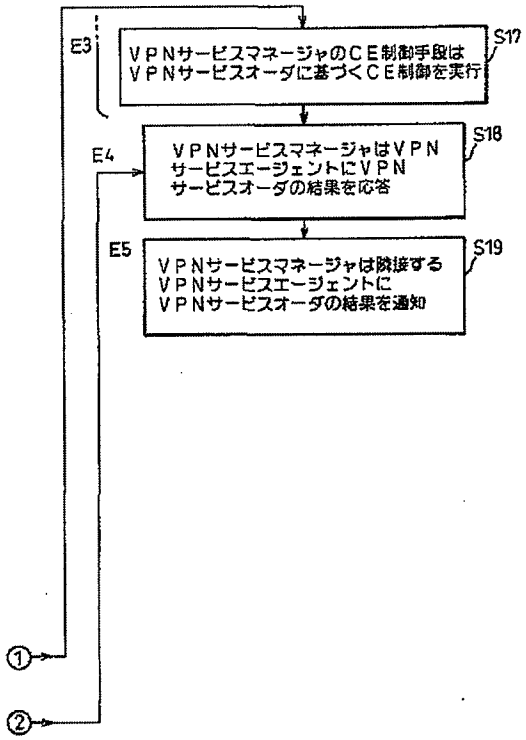
【図１０】

図10　図６での制御シーケンスを説明するためのフローチャート（その１）

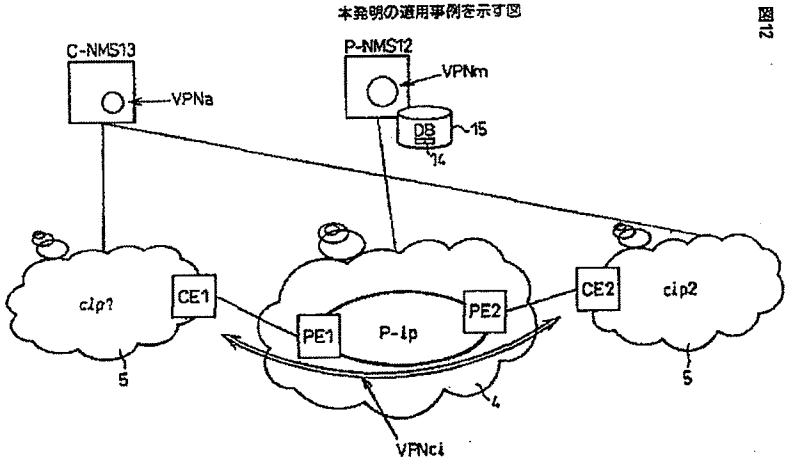


【図１１】

図11　図６での制御シーケンスを説明するためのフローチャート（その２）



【図１２】



【図１３】

図12の適用事例で用いるＶＰＮサービス条件テーブル14の内容を示す図　図13

14

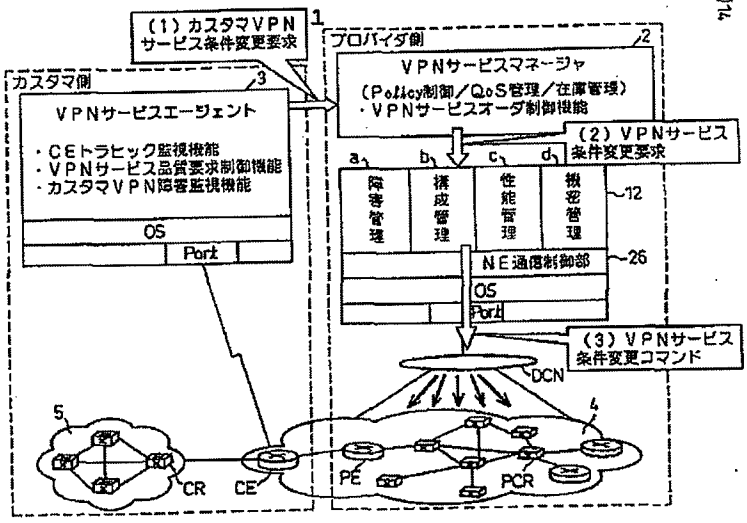
ci-id

ＶＰＮ識別子	ＣＥ識別子（端点Ａ）	ＣＥ識別子（端点Ｚ）
VPNci-id	CE1-id	CE2-id

ＶＰＮサービス条件項目	現在の値	許容値	設定幅
ＶＰＮサービス帯域	bw	bw-max/bw-min	bw△

【図１４】

図１に示すＶＰＮサービス管理システム１の具体的イメージを示す図（その１）　図14

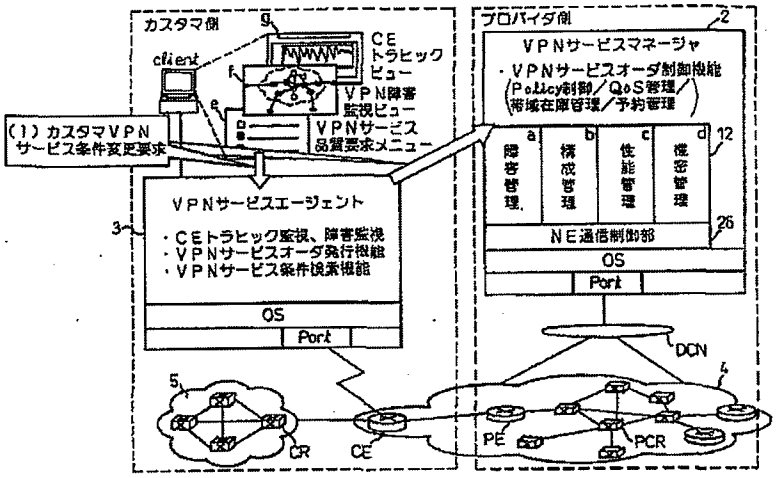


【図２７】

運用管理者への連絡方法を図解的に表す図　図27

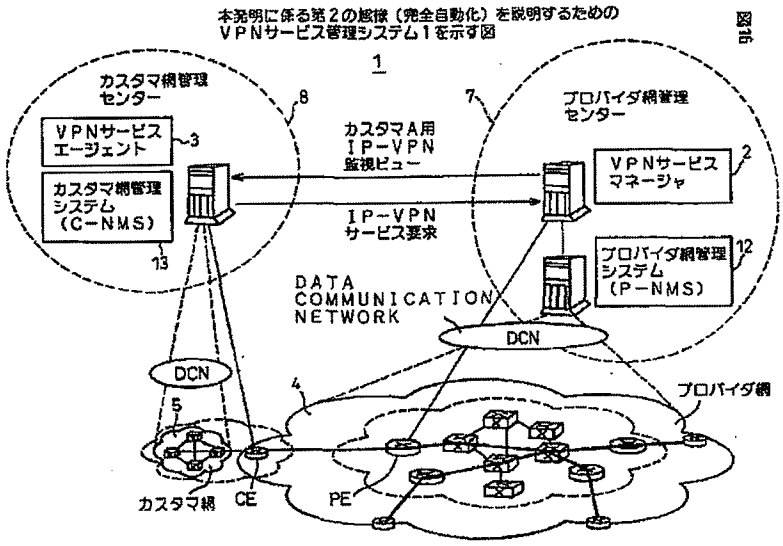
【図１５】

図１に示すＶＰＮサービス管理システム１の具体的イメージを示す図（その２）



【図１６】

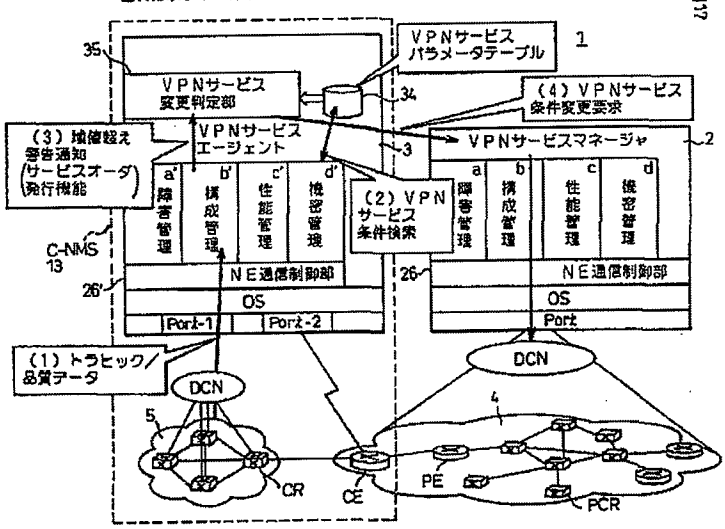
本発明に係る第２の態様（完全自動化）を説明するための
ＶＰＮサービス管理システム１を示す図



【図１７】

図16に示すＶＰＮサービス管理システム１の具体的イメージを示す図

図17



【図１８】

パラメータテーブル34を図解的に示す図

図18

34

VPNサービス条件項目	現在の値	許容値	設定幅
VPNサービス条件1	値1	許容最大／最小値1	幅1
VPNサービス条件2	値2	許容最大／最小値2	幅2
⋮	⋮	⋮	⋮
VPNサービス条件N	値N	許容最大／最小値N	幅N

⇩

レベル	現状値	変更値
レベル1：	Best Effort(BF)	BFから20%up
レベル2：	20% up	50% up
レベル3：	50% up	100% up

【図１９】

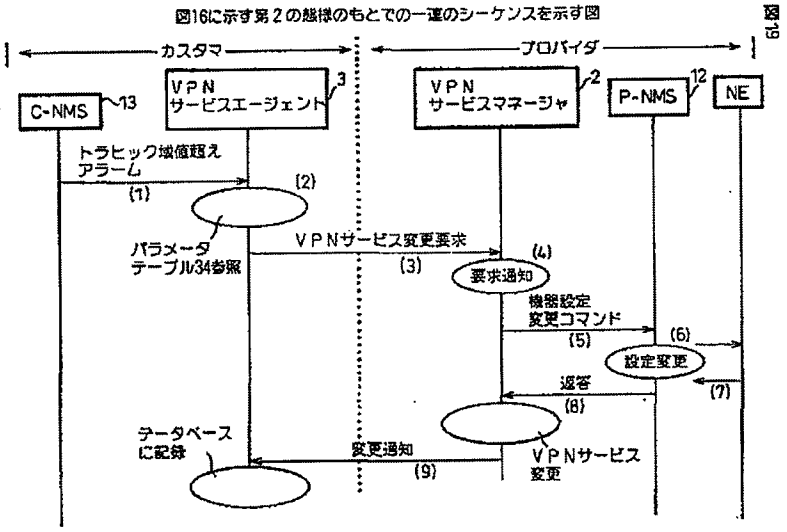
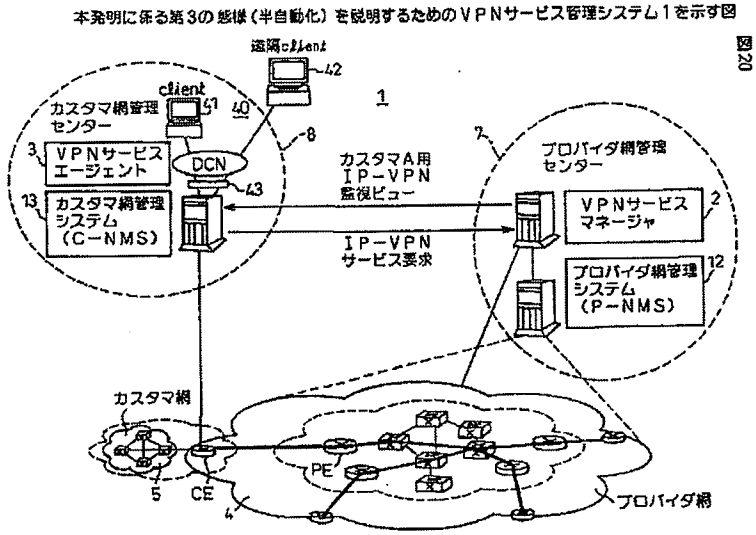


図16に示す第２の態様のもとでの一連のシーケンスを示す図
図19
カスタマ
プロバイダ
C-NMS
13
VPN
サービスエージェント
3
VPN
サービスマネージャ
2
P-NMS
12
NE
トラヒック閾値超え
アラーム
(1)
(2)
パラメータ
テーブル34参照
VPNサービス変更要求
(3)
(4)
要求通知
機器設定
変更コマンド
(5)
(6)
設定変更
(7)
返答
(8)
データベース
に記録
変更通知
(9)
VPNサービス
変更

【図２０】


本発明に係る第３の態様（半自動化）を説明するためのＶＰＮサービス管理システム１を示す図
図20
遠隔client
42
1
client
41
40
カスタマ網管理
センター
8
2
プロバイダ網管理
センター
3
VPNサービス
エージェント
DCN
43
カスタマA用
IP-VPN
監視ビュー
13
カスタマ網管理
システム
(C-NMS)
IP-VPN
サービス要求
VPNサービス
マネージャ
2
プロバイダ網管理
システム
(P-NMS)
12
カスタマ網
PE
5
CE
4
プロバイダ網

【図２１】

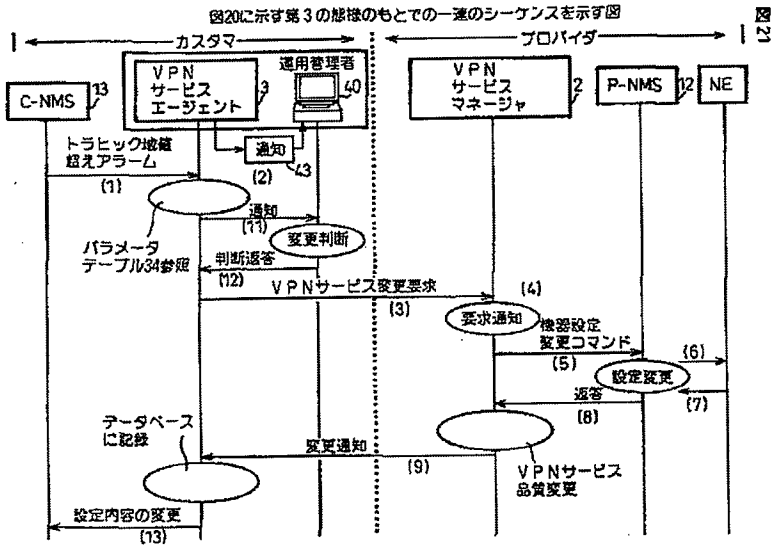
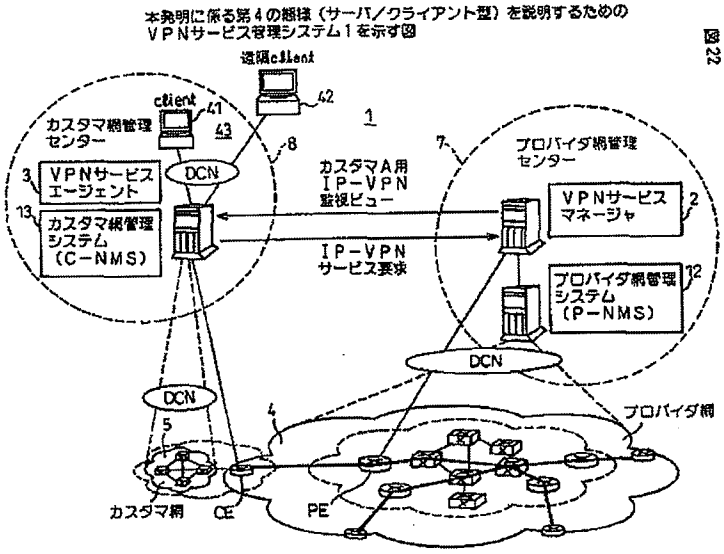


図20に示す第３の態様のもとでの一連のシーケンスを示す図
図21
カスタマ
プロバイダ
VPN
サービス
エージェント
運用管理者
VPN
サービス
マネージャ
C-NMS
P-NMS
NE
トラヒック増減
超えアラーム
(1)
通知
(2)
通知
(11)
変更判断
パラメータ
テーブル34参照
判断返答
(12)
VPNサービス変更要求
(3)
(4)
要求通知
機器設定
変更コマンド
(5)
(6)
設定変更
返答
(7)
(8)
データベース
に記録
変更通知
(9)
VPNサービス
品質変更
設定内容の変更
(13)

【図２２】


本発明に係る第４の態様（サーバ／クライアント型）を説明するための
VPNサービス管理システム１を示す図
図22
遠隔client
client
カスタマ網管理
センター
DCN
VPNサービス
エージェント
カスタマ網管理
システム
(C-NMS)
カスタマA用
IP-VPN
監視ビュー
IP-VPN
サービス要求
プロバイダ網管理
センター
VPNサービス
マネージャ
プロバイダ網管理
システム
(P-NMS)
DCN
DCN
プロバイダ網
カスタマ網
CE
PE

【図２３】

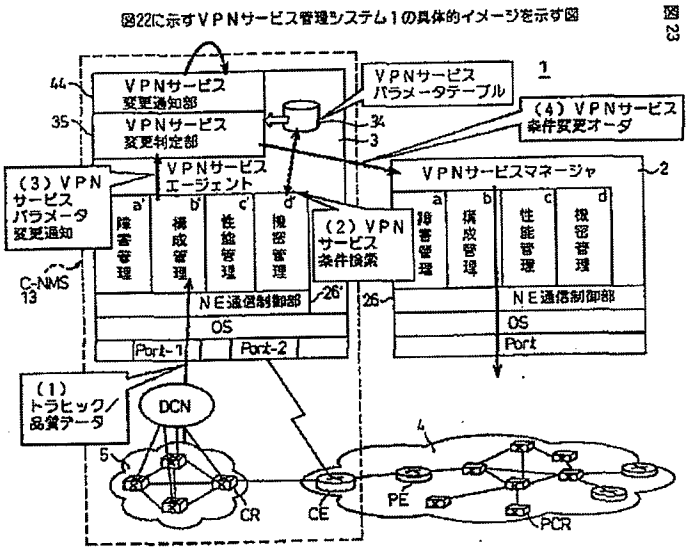


図22に示すVPNサービス管理システム1の具体的イメージを示す図
図23
VPNサービス変更通知部
VPNサービス変更判定部
VPNサービスパラメータテーブル
(4) VPNサービス条件変更オーダ
VPNサービスエージェント
VPNサービスマネージャ
(3) VPNサービスパラメータ変更通知
(2) VPNサービス条件検索
障害管理
構成管理
性能管理
機密管理
NE通信制御部
OS
Port-1
Port-2
Port
C-NMS
(1) トラヒック/品質データ
DCN
CR
CE
PE
PCR

【図２４】

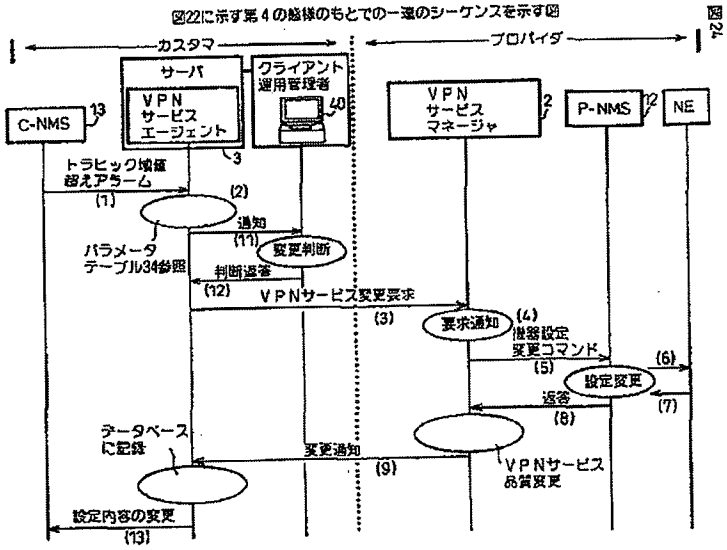
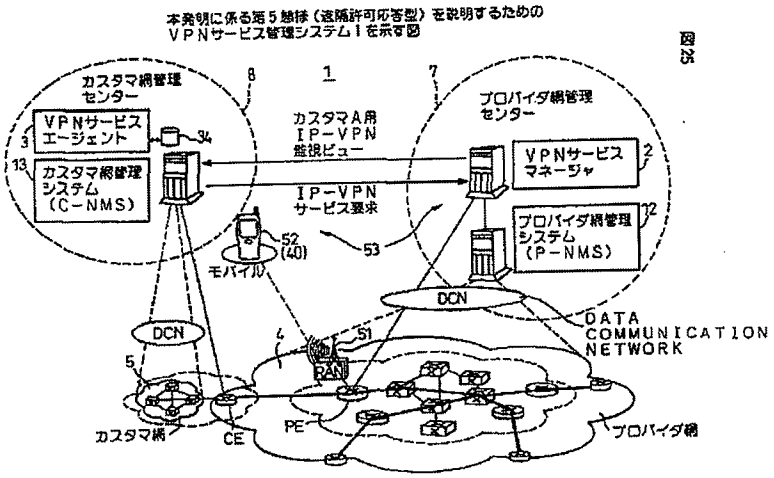


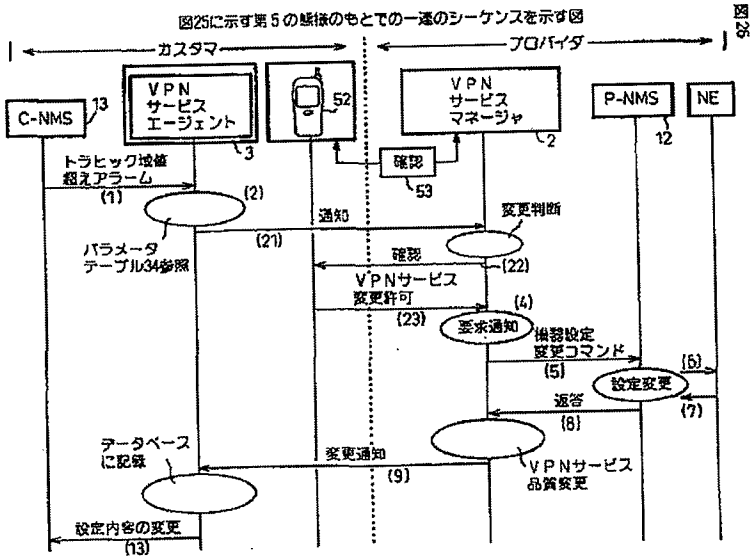
図22に示す第4の態様のもとでの一連のシーケンスを示す図
図24
カスタマ
プロバイダ
サーバ
VPNサービスエージェント
クライアント運用管理者
VPNサービスマネージャ
C-NMS
P-NMS
NE
トラヒック増幅超えアラーム
(1)
(2)
通知
(11)
変更判断
パラメータテーブル34参照
判断返答
(12)
VPNサービス変更要求
(3)
要求通知
(4)
機器設定変更コマンド
(5)
(6)
設定変更
返答
(7)
(8)
データベースに記録
変更通知
(9)
VPNサービス品質変更
設定内容の変更
(13)

【図２５】

本発明に係る第５態様（遮断許可応答型）を説明するための
ＶＰＮサービス管理システム１を示す図

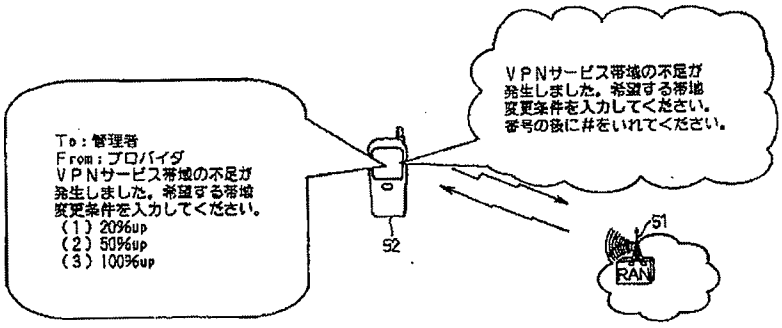


【図２６】



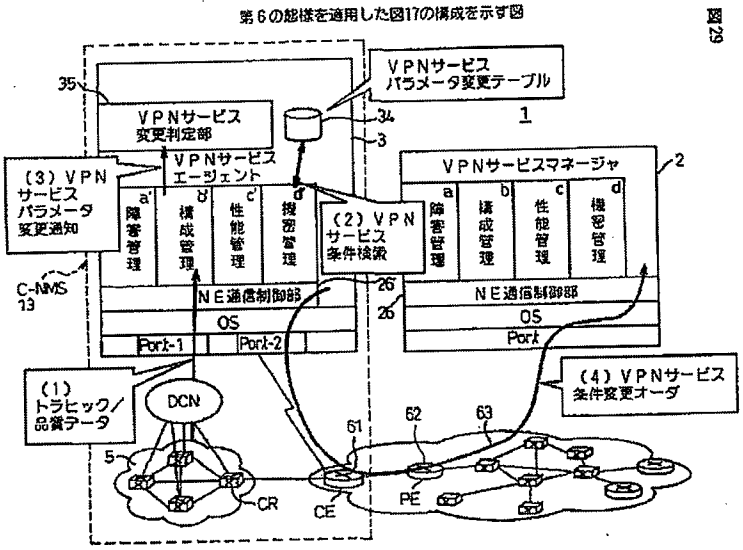
【図２８】

運用管理者との間での事前準備について図解的に表す図　図28



【図２９】

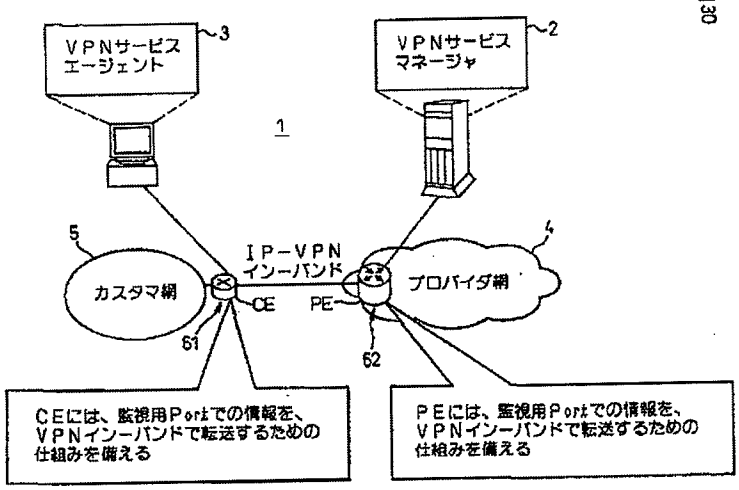
第６の態様を適用した図17の構成を示す図　図29



【図３０】

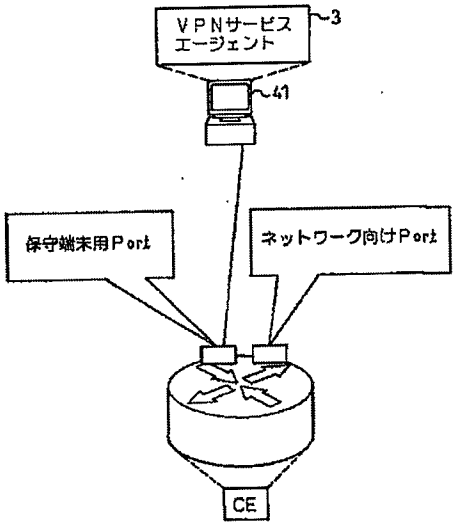
本発明に係るインーバンド手段について説明するための図

図30



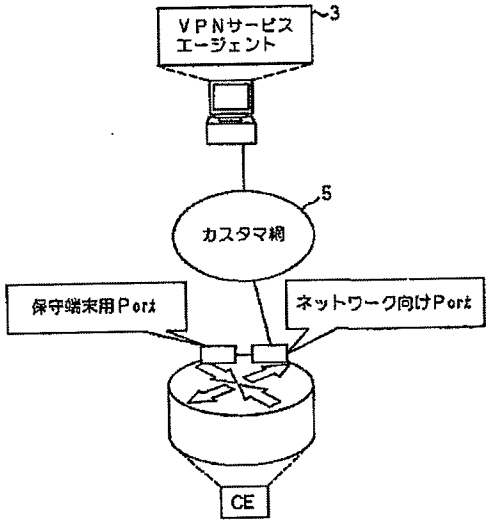
【図３１】

図31　CEとエージェント３との間の第１の接続方法を表す図

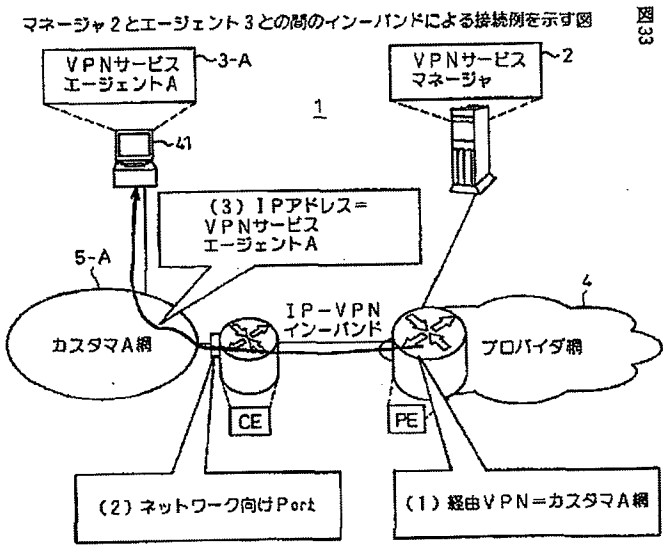


【図３２】

図32　CEとエージェント３との間の第２の接続方法を表す図



【図３３】



フロントページの続き

(72)発明者　小野寺　保子
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　阿部　弘彰
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5K030 GA14 HA08 HC01 HD03 JL07
KA05 KA13 LD17
5K033 BA08 DA01 DB18 DB20
5K051 AA08 AA09 BB02 CC00 CC02
CC08 DD03 DD13 FF07 FF11
FF12 HH27

101560,060

(Document 1)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－282760
（P2001－282760A）
(43)公開日　平成13年10月12日(2001.10.12)

(51)Int.Cl.⁷	識別記号	FI	ﾃｰﾏｺｰﾄﾞ(参考)
G06F 15/177	674	G06F 15/177	674Z 5B045

審査請求 有　請求項の数10 OL （全 18 頁）

(21)出願番号　特願2000－95393(P2000－95393)

(22)出願日　平成12年３月30日(2000.3.30)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　西　耕二
東京都港区五丁目７番１号　日本電気株式会社内

(74)代理人　100082935
弁理士　京本　直樹　（外２名）

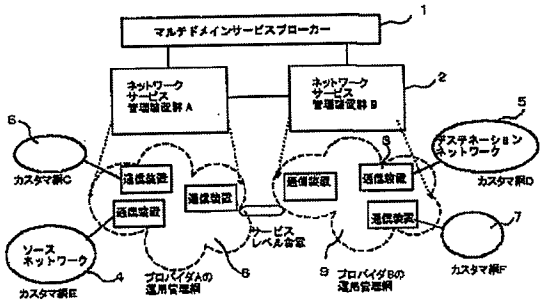
Ｆターム(参考)　5B045 GG02

(54)【発明の名称】　マルチドメインに対応した品質保証型通信サービス提供方式およびサービス提供方法並びにサービス仲介装置

(57)【要約】　（修正有）

【課題】マルチドメインネットワークにおいて品質保証型通信サービスを提供する。

【解決手段】各プロバイダ網の運用管理網に含まれる装置群の管理とサービスオーダ受付けを行うネットワークサービス管理装置２と、複数のプロバイダが締結するための仲介機能を提供するマルチドメインサービスブローカー１とから構成する。マルチドメインサービスブローカーはネットワークサービス管理装置から各プロバイダが提供可能なサービス情報とドメイン情報を収集する手段と、カスタマから通信サービスの要求発生時、要求品質を満足するドメインのネットワークサービス管理装置を抽出し、該当するネットワークサービス管理装置に必要な情報の設定を指示する手段を有する。



1

【特許請求の範囲】

【請求項１】ユーザー端末を収容する複数のカスタマ網を接続し、異なるプロバイダによって運用管理される複数の運用管理網（ドメイン）によって構成される通信ネットワークにおいて、

各プロバイダ網の運用管理網に含まれる装置群を集中管理するとともに、カスタマからのサービスオーダや障害情報の受付けを行うネットワークサービス管理装置と、

前記ネットワークサービス管理装置群の機能的上位層にあって、前記複数のプロバイダが締結するための仲介機能を提供するサービス仲介装置とを含むことを特徴とするマルチドメインに対応した品質保証型通信サービス提供方式。

【請求項２】前記ネットワークサービス管理装置は、各プロバイダが提供可能なサービス情報と、ドメイン情報を前記マルチサービスブローカーに対し出力する手段とを有し、

前記サービス仲介装置は、各ネットワークサービス管理装置からの出力情報を格納し、カスタマから通信サービスの要求発生にともない、当該要求品質を満足するドメインのネットワークサービス管理装置を選択し、必要な情報の紹介と設定を指示する手段を有することを特徴とする請求項１に記載のマルチドメインに対応した品質保証型通信サービス提供方式。

【請求項３】前記ネットワークサービス管理装置は、オペレータから入力される当該プロバイダの提供可能なサービス情報及びプロバイダ運用管理網の構成情報であるドメイン情報を入力するための入出力装置と、

前記入力装置より入力された情報を情報種別毎に記憶する記憶装置、および、各カスタマからのサービス要求に基づき処理コマンドの転送先を決定するワークフローサーバと、

前記ドメイン情報とサービス情報を前記サービス仲介装置に登録を行い、ワークフローサーバと連携して、次の処理の実行主体を決定する帯域ブローカー、および、前記通信装置に必要な情報の処理管理を行う内部処理システムを含むことを特徴とする請求項２に記載のマルチドメインに対応した品質保証型通信サービス提供方式。

【請求項４】前記サービス仲介装置は、前記ネットワークサービス管理装置から、受信したドメイン構成情報と、サービス情報を記憶する記憶装置と、

前記記憶装置に対する情報の書き込み、読み出し等の情報管理を行うとともに、前記帯域ブローカーに対するセキュリティ管理機能を提供するデータ処理装置とを含むことを特徴とする請求項２に記載のマルチドメインに対応した品質保証型通信サービス提供方式。

【請求項５】前記帯域ブローカーと、ワークフローサーバは、カスタマのサービス要求に基づく次の処理の実行主体が外部システムにあるか、内部システムにあるかをロジックに従って決定する手段を有し、

2

次の処理の実行主体が外部システムにある場合、帯域ブローカーがそのドメインを決定する手段と、

次の処理の実行主体が内部システムにある場合、ワークフローサーバがフォワード先の内部処理システムを決定する手段とを含むことを特徴とする請求項３に記載のマルチドメインに対応した品質保証型通信サービス提供方式。

【請求項６】前記サービス仲介装置は、前記サービス記憶部に格納されたサービス状態を参照し、カスタマのサービス要求に基づく次の処理の実行主体が外部システムにあるか、内部システムにあるかを決定する手段と、

次の処理の実行主体が外部システムにある場合、その外部転送先を決定する手段と、

次の処理の実行主体が内部システムにある場合、その転送先の内部処理システムを決定する手段とを含むことを特徴とする請求項３に記載のマルチドメインに対応した品質保証型通信サービス提供方式。

【請求項７】前記内部システムは、それぞれワークフローサーバと接続され、カスタマから受け付けたサービスオーダ情報を管理するカスタマケアサーバと、

プロバイダの運用管理網内部のネットワークリソースを管理する設計サーバと、

あらかじめ記憶されたポリシー情報を読み出すとともに、ベンダ固有の通信装置への設定情報に変換し、サービスを提供するためのプロビジョニングを通信装置に対して行うポリシーサーバと、

プロバイダの運用管理網内にある通信装置、及び、それらを接続する回線の接続構成を含む構成管理、回線断等のネットワーク障害管理機能を提供するネットワーク管理装置のいづれかをを含むことを特徴とする請求項３に記載のマルチドメインに対応した品質保証型通信サービス提供方式。

【請求項８】ユーザー端末を収容する複数のカスタマ網を接続し、異なるプロバイダによって運用管理される複数のドメインによって構成され、

各プロバイダ網の運用管理網に含まれる装置群を集中管理するとともに、カスタマからのサービスオーダや障害情報の受付けを行うネットワークサービス管理装置と、

前記ネットワークサービス管理装置群の機能的上位層にあって、前記複数のプロバイダが締結するための仲介機能を提供するサービス仲介装置とを含むされるマルチドメインに対応した品質保証型通信サービス提供方法であって、

前記サービス仲介装置に対し、各プロバイダのネットワーク管理装置各々が構成情報であるドメイン情報と提供可能なサービス情報とを登録するサービス登録ステップと、

カスタマからの要求を受けて、前記サービス仲介装置とネットワーク管理装置間で要求品質を満たすサービスを提供するためにサービス条件について合意を行い、該当

するドメインのルート情報およびネットワーク管理装置を選択するサービス合意ステップと、
前記ネットワーク管理装置において合意されたサービス条件およびルート情報に基づき通信装置に対し必要なサービスプロビジョニングを行うサービスプロビジョニングステップとを含むことを特徴とするマルチドメインに対応した品質保証型通信サービス提供方法。
【請求項９】前記サービスプロビジョニングステップはさらに、サービスオーダ処理および、ルート設計処理、プロビジョニング処理の各ステップから構成されることを特徴とする請求項８に記載のマルチドメインに対応した品質保証型通信サービス提供方法。
【請求項１０】ユーザー端末を収容する複数のカスタマ網を接続し、異なるプロバイダによって運用管理される複数の運用管理網によって構成されるネットワークにおいて、各プロバイダ網の提供可能なサービス情報と構成情報により複数のプロバイダが締結するための仲介機能を提供する相互接続網におけるサービス仲介装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、異なるプロバイダによって運用管理される複数のドメインをまたがる品質保証型の通信サービスを提供する品質保証型通信サービス提供方式およびサービス提供方法およびサービス仲介装置に関する。
【０００２】
【従来の技術】インターネットの発展に伴い、様々な通信サービス提供事業者（ネットワーク・サービス・プロバイダ）によって通信サービスが提供されてきている。このような中で、異なるプロバイダによって相互接続される複数のネットワークを介して、カスタマが要求する品質をエンドツーエンドに保証する通信サービスを提供することが求められている。
【０００３】このような複数の通信網を接続する方式について、たとえば、特開平０８－２７４８７４号公報の「網相互接続装置及び方法」や、特表平１１－５０１４９５号公報の「トラフィック管理制御用の負荷分散グループのサービス制御点を相互接続する通信リンク」に記載されている。
【０００４】特開平０８－２７４８７４号に記載されている網接続方法では、異なる電気通信網内の要素が相互接続し、網の境界にまたがってサービスの提供を行うインテリジェント網を接続するため、媒介アクセスプロセッサー（ＭＡＰ）を配している。このＭＡＰによって網間でやりとりされるメッセージの変換、検査、及びエミュレーション等を行い、ユーザー側は既存のインターフェイス及びプロトコルを変えることなく、透化な電気通信網を提供するものである。
【０００５】また、特表平１１－５０１４９５号公報記載の発明では、複数のサービス・プロバイダとマルチベンダ装置を取り込んだネットワーク環境において、ネットワーク構成要素が過負荷状態なる問題を解決するため、負荷分散モードで使用する２つのサービス制御点（ＳＣＰ）間に直接、通信リンクによって相互接続機能を提供している。

【０００６】この通信リンクは、負荷分散グループ内で２つのＳＣＰを相互に接続させ、これによって、これらＳＣＰは、それらの輻輳レベルや制御機能についての情報を交換するだけでなく、過負荷ではないＳＣＰへ質問（ｑｕａｒｙ）を送り制御を行う手段を有している。
【０００７】
【発明が解決しようとする課題】しかし、前記のべた従来技術においては、次のような問題点があった。すなわち、特開平０８－２７４８７４号公報に記載の技術では、相互接続された双方の電気通信網をプロビジョニングして、通信サービスを提供するためのオペレーションについて全く考慮されておらず、相互接続ネットワークを介して品質を保証した通信サービスを提供できないという問題点があった。
【０００８】また、特表平１１－５０１４９５号公報記載の発明では、ネットワークが過負荷状態になったときの対応策が提案されているだけであり、その対応を行った場合でも、カスタマに品質を保証した通信サービスを十分提供できない。
【０００９】加えて、相互接続された双方の通信ネットワークをプロビジョニングして、通信サービスを提供するためのオペレーション情報が交換されず、相互接続網を一貫してサービスを提供する機構を備えていない。さらに、通信装置内のＳＣＰにおいて、ＣＰＵ等のリソースを多く使用し、多数の制御機能リストを管理する必要から高機能化する必要があるため、結果としてネットワークに配備される通信装置のコスト増、および処理負荷増をまねくという問題点があった。
【００１０】このように、従来のネットワークにおいては、今後見込まれる多数のネットワーク・サービス・プロバイダによってネットワークが構成され、これらのネットワークで均一な品質を提供することを十分配慮したものではないため、各通信ネットワーク内に、個別に情報をやりとりする為の高機能な装置を備えざるをえず、ネットワークの拡張性、接続の柔軟性に乏しいというような問題点があった。
【００１１】本発明は、このような従来技術の問題点を鑑み、異なるプロバイダによって運用される複数のネットワークを介して、カスタマが要求する品質を保証する通信サービスを提供することを目的とし、あらたに、プロバイダ間の提供可能な情報およびプロバイダ網にまたがるルート設計を行う専用のサービス仲介装置（以下、マルチドメインサービスブローカー）を設けることにより、機能分散をはかり、拡張性の高いシステムを提供するものである。

【００１２】
【課題を解決するための手段】本発明のマルチドメインに対応した品質保証型通信サービス提供方式は、ユーザー端末を収容する複数のカスタマ網を接続し、異なるプロバイダによって運用管理される複数の運用管理網（ドメイン）によって構成されるネットワークにおいて、各プロバイダ網の運用管理網に含まれる装置群を集中管理し、カスタマからのサービスオーダや障害情報の受付けを行うネットワークサービス管理装置と、前記ネットワークサービス管理装置群の機能的上位層にあって、複数のプロバイダが締結するための仲介機能を提供するマルチドメインサービスブローカーとを含んでいる。
【００１３】さらに、前記ネットワークサービス管理装置は、各プロバイダが提供可能なサービス情報と、ドメイン情報を前記マルチサービスブローカーに出力する手段とを有し、前記マルチサービスブローカーにおいては、受信した各ネットワークサービス管理装置からの出力情報を格納し、カスタマから通信サービスの要求を受けて、複数のプロバイダを締結する為の仲介機能を提供し、当該要求品質を満足するドメインのネットワークサービス管理装置を選択し、当該ネットワークサービス管理装置に必要な情報の照会及び設定を指示する手段を有する。
【００１４】
【発明の実施の形態】本発明は、複数のネットワーク・サービス・プロバイダによって運用される運用管理網（ｄｏｍａｉｎ：ドメイン）より構成されるマルチドメインネットワークにおいて、要求元のカスタマから、要求先のカスタマへの通信サービスの提供にあたり、エンド・ツー・エンドに、カスタマが要求する通信品質を保証する通信サービスを提供することを目的とする。
【００１５】そして、各ドメインに設けられたネットワークサービス管理装置間の情報収集と相互の連携を促し、必要とするサービスの仲介を行うマルチドメイン・サービス・ブローカーを導入することにより、異なるドメイン間でもシームレスな通信サービス提供方式を実現するものである。
【００１６】以下に本発明の実施形態の構成について図面を用いて説明する。図１は、本発明の実施の形態のマルチドメインネットワークの構成図であり、複数のカスタマ網と複数のプロバイダ網によって構成されている。このように、マルチドメインネットワークとは、複数のプロバイダの運用管理網を経由し、互いに遠隔地に配置されたカスタマ網が、相互に通信を行うような構成であり、具体的には、企業のネットワークが本社と支店間で構築されている場合や、協力会社がエクストラネットを構築する等のような場合がある。
【００１７】図１に例をあげるように、カスタマ網Ｅとカスタマ網Ｄとの間は、異なるプロバイダの運用管理網であるプロバイダＡの運用管理網８とプロバイダＢの運用管理網９が存在し、運用管理網内には、データの中継転送処理を行う複数の通信装置群３を含んで構成されている。
【００１８】本実施例では、カスタマ網Ｅからカスタマ網Ｄへデータを流すサービスを提供することを例にあげ、カスタマ網Ｅをソースネットワーク４、カスタマ網Ｄをデスティネーションネットワーク５と呼ぶことにする。
【００１９】カスタマが要求する通信品質をソースネットワーク４からデスティネーションネットワーク５まで満足するためには、経由するプロバイダＡ、Ｂの双方がカスタマの要求通信品質を満たすネットワークサービスを提供する必要がある。ここでいう通信品質とは、たとえば、データトラフィックの遅延、揺らぎ、帯域等をさす。従って、プロバイダＡとプロバイダＢとの間に通信品質について合意するためのネゴシエーション（交渉）と連携動作が必要になる。また、各プロバイダ内の通信装置群３の状態などを検出し、具体的な情報の設定／制御を行う為にプロバイダＡ、Ｂの運用管理網の機能的な上位層には、ネットワークサービス管理装置２が各々配備されている。
【００２０】（１）ネットワークサービス管理装置
ネットワークサービス管理装置２は、ネットワークの構成管理、障害管理、性能管理、セキュリティ管理、カスタマ管理、サービス管理等の運用管理を行うものであるが、特に運用管理網内のネットワークの状態を管理し、さらに、カスタマからのサービスオーダや障害申告等の受付けを行っている。
【００２１】図２は、ネットワークサービス管理装置の機能ブロック図である。図に示すように、ネットワークサービス管理装置は、インターネット接続サービス提供の為、あるいは、カスタマ情報やネットワーク情報、プロバイダ情報を管理する為の各種装置群を含んで構成されている。その主な構成を説明すると、プロバイダの運用管理者が、プロバイダが提供できるサービス情報及びプロバイダ運用管理網の構成情報であるドメイン情報を入力するためのキーボード、ディスプレイ等の入出力装置２１、これら入力された情報を情報種別毎に記憶する記憶装置２２、各処理コマンドの内外転送（フォワード）先を決定するワークフローサーバ２４、さらに、ドメイン情報とサービス情報をマルチドメインサービスブローカーに登録を行い、ワークフローサーバと連携し、次の処理の実行主体を決定する帯域ブローカー２３、および、ネットワークサービス管理装置内部の処理を行うカスタマケアサーバ２５、ポリシーサーバ２６、設計サーバ２７、ネットワーク管理装置２８等の内部処理サーバ群から構成されている。
【００２２】以下、ネットワークサービス管理装置２内の記憶装置２２と帯域ブローカー２３、ワークフローサーバー２４および各種内部処理サーバー群の構成につい

て説明する。

【００２３】記憶装置

ネットワークサービス管理装置２内の記憶装置２２は、プロバイダが提供できるサービス情報及びプロバイダ運用管理網の構成情報であるドメイン情報等を記憶格納するものであるが、各種情報の種類毎に設けられた以下の複数の記憶部、すなわち、サービスレベル合意記憶部２２１、ドメイン構成記憶部２２２、ネットワーク構成記憶部２２３、リソース記憶部２２４、ポリシー記憶部２２５、サービス記憶部２２６とを備えている。

【００２４】ここで、サービスレベル合意記憶部２２１とは、詳細は後述するが、プロバイダＡがプロバイダＢと通信サービスに関して合意の上、締結した情報を記憶するものである。この締結情報には、プロバイダＡとプロバイダＢの双方の運用管理網を連結する通信装置、および通信装置を連結する回線のタイプと識別子、サービスタイプ、データトラフィックのプロファイル情報、締結有効時間等を含む。また、データトラフィックのプロファイル情報とは、帯域情報と通信品質を含み、例えば通信データのトラフィックが、１０Ｍｂｐｓ以下の場合は高優先の通信品質を提供し、１０Ｍｂｐｓ以上の場合は通信データを破棄するというような情報が記述されている。

【００２５】ドメイン構成記憶部２２２は、カスタマに通信サービスを提供するためのドメイン構成情報を記憶している。ドメイン構成情報とは、プロバイダ運用管理網の構成情報である。たとえば、図１の例では、カスタマ網のソースネットワークからデスティネーションネットワークまでは、プロバイダＡ運用管理網とプロバイダＢ運用管理網を経由しているが、この場合、プロバイダＡ運用管理網とプロバイダＢ運用管理網の連結をサービス提供に必要なプロバイダ網として、ドメイン構成記憶部２２２は記憶している。

【００２６】ネットワーク構成記憶部２２３は、プロバイダ運用管理網内にある通信装置群３、および、その通信装置群３を連結する回線情報等を記憶している。リソース記憶部２２４は、プロバイダ運用管理網内にある通信装置３、および、その通信装置３が有する全リソース量、使用済みリソース量、残余リソース量等の情報を記憶する。ここで、一般に、リソースとは、通信装置３のＣＰＵ能力、メモリ量、回線の帯域を表現する。本実施例では、回線帯域についてリソースを記憶するが、それ以外の情報を含むものであってよい。

【００２７】ポリシー記憶部２２５は、プロバイダ運用管理網内の通信装置３に対して設定する情報をポリシーとして記憶する。ここで、ポリシーとは、カスタマに通信サービスを提供する為に通信装置３に設定すべき情報をオペレータにとってわかりやすく表現したものであり、通信装置３のベンダに依存しない表現で記述したものである。例えば、図１を参照すると、カスタマ網Ｅからカスタマ網Ｄまで高優先の通信データを１０Ｍｂｐｓまで保証する、という表現がここでいうポリシーの一例である。サービス記憶部２２６は、カスタマ情報、及び、カスタマから受け付けたサービス情報を記憶する。例えば、カスタマ網Ｅからカスタマ網Ｄまで高優先の通信データを１０Ｍｂｐｓまで保証、という内容を表現するサービスオーダ情報を記憶する。

【００２８】帯域ブローカー

次に帯域ブローカーの構成について説明する。帯域ブローカー２３はプログラム制御により動作するデータ処理機能を有するシステムであり、外部システム通信手段２３３、セキュリティ管理手段２３４、サービスレベル合意管理手段２３１、ドメインルート管理手段２３２、内部システム通信手段２３５とを備える。

【００２９】ここで、外部システム通信手段２３３は、外部システムである他のネットワークサービス管理装置群２、及び、マルチドメインサービスブローカー１と接続され、この外部システムと通信するためのインタフェースを提供する。セキュリティ管理手段２３４は、外部システムとの通信に際して、内部システムのセキュリティを確保する。例えば、外部システムとの接続後に、外部システムから認証情報を受信し、認証成功後に情報交換を行う。

【００３０】サービスレベル合意管理手段２３１は、プロバイダ間で締結、合意したサービス情報をサービスレベル合意記憶部２２１に登録するとともに、情報を管理する。また、入出力装置２１に対してサービスレベル合意情報を登録、編集、削除するためのインタフェースを提供する。

【００３１】ドメインルート管理手段２３２は、カスタマに通信サービスを提供するために必要なドメインの連結情報をドメイン構成記憶部２２２に登録すると共に、管理する。内部システム管理手段２３５は、帯域ブローカー２３とワークフローサーバ２４が通信するためのインタフェースを提供する。

【００３２】ワークフローサーバー

ワークフローサーバ２４は、同様に、プログラム制御によりデータ処理を行う機能を有するシステムであり、帯域ブローカー２３、及び、カスタマケアサーバ２５、設計サーバ２７、ポリシーサーバ２６、ネットワーク管理装置２８と各々接続される。ワークフローサーバ２４は、プロバイダが定義したワークフロー、または、オペレーションフローに従って、各サーバに必要な処理命令を転送すると共に、その進捗状況を管理する。

【００３３】内部処理サーバー群

次に、その他、通信装置を含むネットワークに関し、具体的な設定処理、制御を行う為の各種内部処理サーバ群である、カスタマケアサーバ２５、ポリシーサーバ２６、設計サーバ２７、ネットワーク管理装置２８について説明する。

【００３４】カスタマケアサーバ２５は、プログラム制御により動作するデータ処理機能を有するシステムであり、ワークフローサーバ２４と接続されている。カスタマから受け付けたサービスオーダ情報を管理し、カスタマ情報、および、カスタマから受け付けたサービス情報をサービス記憶部２２６に登録を行う。また、入出力装置２１に対してサービス情報を登録、編集、削除するための前記サービス記憶部２２６に対するインタフェースを提供する。

【００３５】設計サーバ２７は、同じくプログラム制御により動作するデータ処理機能を有するシステムであり、ワークフローサーバ２４と接続されている。本サーバ２７は、プロバイダの運用管理網内部のネットワークリソースを管理し、本実施例の場合は、通信回線の全帯域、使用済み帯域、残余帯域を管理している。

【００３６】リソースの使用状況が変更された場合、リソース記憶部２２４内の情報を更新し、プロバイダの運用管理網内部のトポロジー情報を参照するために、ネットワーク構成記憶部２２３から情報を読み出し、常に最新のネットワークリソース情報を管理している。また、リソース使用計画の出力として、ポリシー情報をポリシー記憶部２２５に登録する処理も行う。

【００３７】ポリシーサーバ２６は、プログラム制御により動作するデータ処理機能を有するシステムであり、ワークフローサーバ２４と接続される。ポリシー記憶部２２５に記憶されたポリシー情報を読み出すと共に、ベンダ固有の通信装置３への設定情報に変換する。次に、サービスを提供するためのプロビジョニングを通信装置３に対して行う。

【００３８】ネットワーク管理装置２８は、プログラム制御により動作するデータ処理機能を有するシステムであり、ワークフローサーバ２４と接続される。プロバイダの運用管理網内にある通信装置３、及び、それらを接続する回線の接続構成を含む構成管理、回線断等のネットワーク障害管理機能を提供する。

【００３９】以上述べた構成によって、ネットワークサービス管理装置は、プロバイダ間の接続の仲介機能を提供するマルチドメインサービスブローカーに、必要な情報を提供するとともに、前記マルチドメインサービスブローカーから通知された情報に基づき、通信装置に対する具体的な設定、制御動作を行う機能を実現することができる。

【００４０】（２）マルチドメインサービスブローカー
次に、マルチドメインサービスブローカー１について説明する。ネットワークサービス管理装置群２の機能的上位層にマルチドメインサービスブローカー１は配置され、複数のプロバイダが締結するための仲介機能を提供する。

【００４１】図３は、マルチドメインサービスブローカーの機能ブロック図である。図３を参照すると、マルチドメインサービスブローカー１は、キーボードやディスプレイ等から構成される入出力装置１１、プログラム制御により動作するデータ処理装置１３と、情報を記憶する記憶装置１２から構成される。

【００４２】入出力装置１１は、セキュリティ管理手段１３３と接続され、マルチドメインサービスブローカー１が管理するプロバイダのネットワークサービス管理装置群２と通信するための認証情報等を登録、変換、削除の操作を行うことができる。記憶装置１２は、ドメイン構成記憶部１２１とサービス記憶部１２２を備える。ドメイン構成記憶部１２１は、マルチドメインサービスブローカー１が管理するプロバイダの運用管理網とその接続構成を記憶する。本実施例の場合、プロバイダＡとプロバイダＢの運用管理網がマルチドメインサービスブローカー１の管理対象である。

【００４３】サービス記憶部１２２は、各プロバイダが提供するサービスを記憶する。本実施例の場合、プロバイダＡ、Ｂと共に高品質、中品質、低品質の通信サービスを提供する。データ処理装置１３は、ドメイン構成管理手段１３１、セキュリティ管理手段１３３、サービス管理手段１３２、外部システム通信手段１３４をおのおの備える。

【００４４】ドメイン構成管理手段１３１は、マルチドメインサービスブローカー１が管理対象とするプロバイダの運用管理網に関するオペレーションを提供し、ドメイン構成記憶部１２１にドメイン構成情報を登録、編集、削除する機能を提供する。マルチドメインサービスブローカー１は、プロバイダから登録申告のあったドメイン情報をドメイン構成管理手段１３１経由でドメイン構成記憶部１２１に記憶する。

【００４５】セキュリティ管理手段１３３は、マルチドメインサービスブローカー１が接続されるネットワークサービス管理装置群２の認証処理を行う。ネットワークサービス管理装置群２との接続を確立後に認証情報を受信し、セキュリティ管理手段１３３によって認証された場合、ネットワークサービス管理装置２と、その後のデータ交換を行う。

【００４６】サービス管理手段１３２は、各プロバイダが提供できるサービスを管理すると共に、サービス記憶部１２２にサービス情報の登録、編集、削除を実行するものである。外部システム通信手段１３４は、マルチドメインサービスブローカー１と各プロバイダのネットワークサービス管理装置群２が通信するためのインタフェースを提供する。

【００４７】次に本発明の動作について説明する。本発明では、異なるプロバイダが操作するネットワークサービス管理装置群２、及び、マルチドメインサービスブローカー１が連携することによって、マルチドメインにまたがる品質保証型の通信サービスをカスタマに提供する。連携のためにキーとなるのが、ネットワークサービ

ス管理装置群２内にある帯域ブローカーとマルチドメインサービスブローカー１である。

【００４８】本発明のマルチドメインに対応した通信サービス提供方式の手順は、（ア）サービス登録段階、（イ）サービス合意段階、（ウ）サービスプロビジョニング段階、の主に三段階に分類される。以降、図を参照して本発明の実施形態の動作について説明する。

【００４９】（ア）サービス登録段階

サービス登録段階では、各プロバイダのネットワークサービス管理装置群２がマルチドメインサービスブローカー１に対して、運用管理網が提供できるサービス情報とドメイン情報を登録するフェーズである。この段階の処理により、マルチドメインサービスブローカー１では、接続する全ての運用管理網のサービス情報とプロバイダ情報を収集し、管理することができる。

【００５０】本サービス登録段階の処理について具体的に説明すると、各プロバイダの運用管理者であるオペレータは、入出力装置１１を使用して、プロバイダが提供できるサービス情報、及び、プロバイダ運用管理網の構成情報であるドメイン情報を入力する。こうして入力されたプロバイダの提供可能なサービス情報、ドメイン情報は、外部システム通信手段２３３を介してマルチドメインサービスブローカー１に送信される。

【００５１】また、本実施の形態では、各プロバイダのサービス情報および、ドメイン情報をオペレータから入力する実施形態について説明するが、当該情報の入力を、あらかじめプログラムした条件により自動的に設定入力するものであっても、カスタマや各ネットワークサービス管理装置間で通知されるメッセージ情報により自動的に設定更新するように構成することも可能である。

【００５２】マルチドメインサービスブローカー１は、外部システム通信手段１３４を介して、各プロバイダから提供可能なサービス情報、ドメイン情報を受信すると、各々、記憶装置１２の中のサービス情報記憶部１２２とドメイン構成記憶部１２１に格納しておく。

【００５３】次に上記述べたサービス登録段階の動作を図４を用いて説明する。図４は、本発明のサービス登録段階の手順を示すフローチャートである。

【００５４】まず、一連の動作の前にネットワークサービス管理装置２は、マルチドメインサービスブローカー１と管理情報通信用のコネクションを確立し、確立後、ネットワークサービス管理装置２はセキュリティ管理手段２３４によって認証情報を送信し、マルチドメインサービスブローカー１間で管理情報交換の許可を受け、論理的な通信パスを形成しておく。

【００５５】次に、運用管理者であるオペレータは、入出力装置２１を使用してプロバイダＡが提供できるサービス情報、及び、プロバイダＡ運用管理網の構成情報であるドメイン情報を入力する（ステップＡ１）。入力されたサービス情報、ドメイン情報は、外部システム通信手段２３３を介してマルチドメインサービスブローカー１に送信される（ステップＡ２）。

【００５６】マルチドメインサービスブローカー１は、外部システム通信手段１３４を介してサービス情報、ドメイン情報を受信すると（ステップＡ３）、その情報の内容チェックを行い（ステップＡ４）、文法的に正しい場合、それらの情報をそれぞれ、サービス情報記憶部１２２とドメイン構成記憶部１２１に格納する（ステップＡ５）。

【００５７】こうして、マルチドメインサービスブローカー１は、複数のプロバイダの各ネットワークサービス管理装置からドメイン情報、サービス情報を収集し、内部に登録する。

【００５８】（イ）サービス合意段階

次に、カスタマへの具体的な通信サービスの提供にあたり、相互接続するプロバイダで同等の品質の通信サービスを提供する為、運用管理網間のサービス合意するサービス合意段階について説明する。

【００５９】このサービス合意段階とは、カスタマからの要求をうけて、マルチドメインネットワーク内を一貫した通信品質で通信サービスを提供できるように、マルチドメインサービスブローカー１および、ネットワークサービス管理装置群とでネゴシエーションを行い、要求品質を満たす適切なドメインを選択し通話ルートの決定を行ってサービスレベルの合意を行う処理に相当する。

【００６０】ここでいう、サービスレベルの合意について、その必要性について説明する。各プロバイダは、通信品質のレベルをエラーレートあるいは、遅延値などの種々のパラメータによって通信サービスの品質を指定することができ、提供可能な品質およびその指定方法は一般に相違する。たとえばあるプロバイダにおいて、品質の高い順に３レベル、たとえば、ＧＯＬＤ、ＳＩＬＶＥＲ、ＢＲＯＮＺＥという呼称で、カスタマに指定させるものであっても、別のプロバイダにおいては、異なるエラーレートの値やレベル数（たとえば、Ａ、Ｂ、Ｃ、Ｄ）等のパラメータで、カスタマに品質を指定させる場合がある。

【００６１】よって、カスタマによって要求される品質が、マルチドメインサービスネットワーク内で等しく保たれるためには、それぞれのプロバイダ内で、どのようなサービスのレベルに相当するか対応付けを行い、相互に合意しておく必要がある。このとき、各ドメイン間のサービス合意の仲介者としての役割を果たすのが、マルチドメインサービスブローカー１である。

【００６２】本サービス合意段階の動作について簡単に説明する。まず、あるプロバイダのオペレータが、ネットワークサービス管理装置２の入出力装置２１を用いてサービスレベル合意をしたい条件であるサービス情報を入力する。入力されたサービス情報は、外部システム通信手段２３３を介して、マルチドメインサービスブロー

カー１へ送信される。マルチドメインサービスブローカー１はサービス情報を受信すると、サービス管理部１３２によってサービス記憶部１２２を検索して、条件を満足するドメインＩＤを獲得する。

【００６３】次に、マルチドメインサービスブローカー１は、ドメインＩＤをキーにして、当該ドメインのドメイン構成情報をドメイン構成記憶部１２１から読み出し、要求元のネットワークサービス管理装置群２内の帯域ブローカー２３へ応答としてドメイン情報を送信する。

【００６４】応答を受信したネットワークサービス管理装置において、マルチドメインサービスブローカー１から、あるドメインが通知されると、オペレータは入出力装置２１を使用してサービスレベル合意情報を帯域ブローカー２３に入力する。このとき、このサービスレベル合意情報は、ネットワークサービス管理装置２の外部システム通信部２３３を介して、マルチドメインサービスブローカー１から紹介された隣接ドメインの帯域ブローカー２３宛にメッセージ送信され、隣接ドメインにおいてもサービスレベル合意情報が登録される。以上の処理により、プロバイダの運用管理網の間で、相互接続に関する合意がなされる。

【００６５】この合意情報には、相互接続する通信装置、回線、サービスタイプ、帯域等が含まれる。こうしてサービス合意段階の処理によって、異なるプロバイダ間を同一の品質で通信サービスを提供するための取り決めについて情報の交換と対応づけが行われて、プロバイダ間でサービスレベルの合意がなされることになる。

【００６６】次に、図５を参照してサービス合意段階を具体的に説明する。サービス合意は、異なるプロバイダ間で締結され、運用管理網の相互接続に関する規約である。

【００６７】プロバイダＡのオペレータ（以降、オペレータＡ）は、入出力装置２１を用いてサービスレベル合意をしたい条件であるサービス情報を入力する。サービス情報には、高優先、中優先、低優先のサービス分類等の情報が含まれる。入力されたサービス情報は、外部システム通信部２３３を介して、マルチドメインサービスブローカー１へ送信される（ステップＢ１）。

【００６８】マルチドメインサービスブローカー１がサービス情報を受信すると、サービス管理部１３２がサービス記憶部１２２を検索して、条件を満足するドメインＩＤを獲得する（ステップＢ２）。

【００６９】そして、ドメイン構成管理部１３１は、ドメインＩＤをキーにして該ドメイン情報をドメイン構成記憶部１２１から獲得する。次に、マルチドメインサービスブローカー１は、外部システム通信部１３４を介して、プロバイダＡの帯域ブローカー２３（以降、帯域ブローカーＡ）へ応答を送信する。帯域ブローカー２３がドメイン情報を受信すると、入出力装置２１へ出力する。本実施例の場合、プロバイダＢのドメイン（以降、ドメインＢ）が紹介される（ステップＢ３）。

【００７０】オペレータＡは、ドメインＢを指定して、サービスレベル合意情報を入力する。サービスレベル合意情報には、高優先、中優先、低優先等のサービスクラスと要求する通信品質情報を含む。本実施例では、帯域情報を入力する。サービスレベル合意情報は、外部システム通信手段２３３を介して、プロバイダＢの帯域ブローカー２３（以降、帯域ブローカーＢ）に送信される（ステップＢ４）。

【００７１】ただし、これら一連の処理の送信前に帯域ブローカーＡは帯域ブローカーＢと管理情報交換用のコネクションを確立して認証を受ける。認証は、セキュリティ管理部２３４が行う。

【００７２】帯域ブローカーＢがサービスレベル合意情報を受信すると、データ内容をチェックする。文法的に誤りがない場合、帯域ブローカーＢ内のサービスレベル合意管理部２３１（以降、サービスレベル合意管理部Ｂ）は、サービスレベル合意記憶部２２１からドメインＡとドメインＢとの間の残余リソース量、高優先、中優先、低優先等のサービス情報を取得する。合意可能な場合、外部システム通信部Ｂを介して、帯域ブローカーＡに対して応答を送信すると共に、プロバイダＡと合意したサービス合意情報をサービスレベル合意記憶部Ｂに登録する（ステップＢ５）。

【００７３】帯域ブローカーＡが応答を受信して、サービスレベル合意要求が受容された場合、該合意情報をサービスレベル合意記憶部Ａに登録する（ステップＢ６）。

【００７４】以上の処理により、プロバイダＡとプロバイダＢの運用管理網の間で、相互接続に関する合意がなされる。合意情報は、相互接続する通信装置、回線、サービスタイプ、帯域等を含む。

【００７５】（ウ）サービスプロビジョニング段階

次に、サービスプロビジョニング段階を実行する。サービスプロビジョニングは、カスタマからのサービスオーダに基づいて、複数のプロバイダの運用管理網を介したカスタマ網間のサービスを開通するため、通信装置に対する情報の設定制御を含むオペレーションを行うステップである。

【００７６】このサービスプロビジョニング段階とは、サービスオーダ処理、ルート設計処理、プロビジョニング処理の三段階にさらに分類される。そして、これらの処理はそれぞれ、カスタマケアサーバ、設計サーバ、ポリシーサーバにより主に実行される。

【００７７】これらのサーバ群を通信サービス提供のためのオペレーションフローに従って制御するのが、ワークフローサーバ２４であり、各ドメインのネットワークサービス管理装置２内にあるカスタマケアサーバ２５、設計サーバ２７、ポリシーサーバ２６、ワークフローサ

ーバ２４等を連携動作させるのが、ワークフローサーバ２４である。

【００７８】すなわち、サービスオーダ処理とは、カスタマケアサーバ２５において、カスタマからサービスオーダ情報を受付し管理すると共に、サービス記憶部２２６に登録する処理をさし、ルート設計処理とは、プロバイダの運用管理網内部のネットワークリソースを管理する設計サーバ２７において、通信回線の全帯域、使用済み帯域、残余帯域を管理し、リソースの使用状況によって具体的なルートを決定する処理をいう。さらに、プロビジョニング処理とは、ポリシーサーバ２６によって記憶部２２５に記憶されたポリシー情報を読み出すと共に、ベンダ固有の通信装置への設定情報に変換する。次に、サービスを提供するためのプロビジョニングを通信装置３に対して行う制御処理をいう。

【００７９】以下に、サービスプロビジョニング段階におけるサービスオーダ処理、ルート設計処理、プロビジョニング処理の処理例を記述する。

【００８０】まず、サービスオーダ処理において、カスタマはプロバイダＡに対してサービスオーダを要求し、このサービスオーダ情報は、オペレータＡがネットワークサービス管理装置２の入出力装置２１を使用してカスタマケアサーバ２５に登録を行う。またカスタマケアサーバ２５は、オペレータからの入力情報をサービス記憶部２２６に記憶する。

【００８１】次に、ルート設計処理では、ドメイン間接続のルート設計と、ドメイン内のルート設計処理を行う。前者は、カスタマ網のソースネットワークからデスティネーションネットワークまでを経由するプロバイダの運用管理網の連結を計算する処理であり、マルチドメインサービスブローカー１が実行する。後者は、プロバイダの運用管理網内において、通信装置３の連結を計算する処理であり、設計サーバ２７が実行する。

【００８２】まず、ドメイン間接続のルート設計をするために、ネットワークサービス管理装置２の帯域ブローカー２３が外部システム通信手段２３３を介して、マルチドメインサービスブローカー１に要求メッセージを送信する。

【００８３】マルチドメインサービスブローカー１がドメイン間のルート設計を実行し、応答がマルチドメインサービスブローカー１から、帯域ブローカー２３に送信される。

【００８４】次に、設計サーバ２７が要求された通信品質を満足するドメイン内部のルートを設計する。設計サーバ２７が実行したドメイン内ルート設計の結果は、リソース記憶部２２４と、ポリシー記憶部２２５に書き込まれる。

【００８５】リソース記憶部２２４には、設計によって新規に割り当てられたネットワークリソース情報を更新する。ポリシー記憶部２２５には、ネットワーク内の通信装置３に設定するためのコンフィグレーションデータをポリシーとして書き込む。

【００８６】次に、帯域ブローカー２３のサービスレベル合意管理手段２３１が、サービスレベル合意記憶部２２１を参照して、カスタマの要求するサービス情報が、プロバイダＡとプロバイダＢとの間で合意したサービスに収容できるか否かをチェックする。

【００８７】収容できる場合、ネットワークサービス管理装置２は、外部システム通信手段２３３を介して、隣接ドメインの帯域ブローカー１へサービスプロビジョニング要求メッセージを送信する。

【００８８】隣接ドメインの帯域ブローカー２はサービスプロビジョニング要求を受信すると、当該隣接ドメインのネットワークサービス管理装置の設計サーバ２７が要求された通信品質を満足するドメイン内部のルートを計算する。

【００８９】次に、隣接ドメインの帯域ブローカー２が、設計結果として要求元の帯域ブローカーに対してサービスプロビジョニング応答を送信する。こうして、サービスオーダ処理、ルート設計処理によって、サービスオーダーの登録と、ドメイン内およびドメイン間のルート設計が実行されることになる。

【００９０】第三のプロビジョニング処理において、上記設計されたルート情報等にもとづき、該当する通信装置に具体的な構成情報の設定、制御を行う。すなわち、ポリシーサーバ２６はサービスを提供するための通信装置３へのコンフィグレーションデータをポリシー記憶部２２５から読み出す。ここで、ポリシーサーバ２６がプロビジョニングを行う対象は、プロバイダの運用管理網である。

【００９１】次に、帯域ブローカー２は、ドメイン構成記憶部２２２から該サービスを提供するために経由するドメインの連結情報を取得し、隣接ドメインの帯域ブローカー２に対してサービスプロビジョニングの要求メッセージを送信する。

【００９２】隣接ドメインの帯域ブローカー２がサービスプロビジョニングの要求メッセージを受信すると、ポリシーサーバ２６が、該サービスのポリシーデータをポリシー記憶部２２５から読み出す。次に、隣接ドメインの運用管理網内で、サービスに関係する通信装置３に対してプロビジョニングを実行する。

【００９３】次に、隣接ドメインの帯域ブローカー２３は、要求元の帯域ブローカー２３に対してサービスプロビジョニング応答メッセージを送信する。

【００９４】帯域ブローカー２３が隣接ドメインからサービスプロビジョニング応答メッセージを受信すると処理を終了し、複数のドメインを介した通信サービスが提供される。

【００９５】次に、上記処理を図６、７を参照してサービスプロビジョニング段階について詳細に説明する。図

６は、本発明のサービスプロビジョニング段階の動作を示すフローチャートである。図７は、本発明のサービスの状態遷移図である。

【００９６】図６のフローチャートにおいて、複数の実行ブロックがある。上側にある内外フォワード先決定（ステップＣ１）は帯域ブローカー２３、または、ワークフローサーバ２４が行う処理である。

【００９７】また、左側の外部フォワード先決定（ステップＣ２）、アドミッションコントロールデシジョン（ステップＣ５）、サービスプロビジョニング応答送信（ステップＣ３）、サービスプロビジョニング応答受信（ステップＣ４）、サービスプロビジョニング要求送信（ステップＣ６）、サービスプロビジョニング要求受信（ステップＣ７）は、帯域ブローカー２３が行う処理である。

【００９８】ドメイン間ルート設計（ステップＣ８）は、マルチドメインサービスブローカー１が行う。右側の内部フォワード先決定（ステップＣ９）は、ワークフローサーバ２４が行う。サービス受け付け（ステップＣ１０）はカスタマケアサーバ２５、ドメイン内ルート設計（ステップＣ１１）は設計サーバ２７、プロビジョニング（ステップＣ１２）はポリシーサーバ２６がそれぞれ実行する。

【００９９】また、サービスプロビジョニング段階では、各ドメインにおいてカスタマに提供するサービスの状態を管理する。図７にサービスの状態遷移図を示す。

【０１００】始めに、カスタマはプロバイダＡに対してサービスオーダを要求する。サービスオーダには、カスタマ網のロケーション情報、通信品質情報が含まれる。本実施例では、カスタマ網Ｅ、カスタマ網Ｄ、高優先等のサービスクラス、要求帯域が申告される。

【０１０１】以下の説明において、プロバイダＡにおいて、受け付けたサービスオーダーについてマルチドメインサービスブローカー１が所望の通信サービスを提供するプロバイダとしてプロバイダＢを選定する場合について説明する。ここで、対応各機能装置、ブロックの付番は、以上、図２、３等で述べた構成と同一のものであるが、おのおの各プロバイダに対応してＡ、Ｂの添え字をつけて表記するものとする。

【０１０２】プロバイダＡにおいて、受け付けたサービスオーダ情報は、オペレータＡが入出力装置２１Ａを使用してカスタマケアサーバ２５Ａに登録する。カスタマケアサーバ２５Ａはデータの文法チェックを行い、正しい場合、サービス記憶部　２２６Ａに格納する（図６のステップＣ１０）。また、サービス状態をＡｃｃｅｐｔｅｄとして格納する（図７の状態Ｄ１）。

【０１０３】次に、ワークフローサーバ２４Ａにおいて内外フォワード先決定を行う（ステップＣ１）。

【０１０４】内外フォワード先決定は、図９に示すようにサービス記憶部２２６Ａに格納されるサービス状態を参照し、プログラム制御としてサーバ、あるいは、システムに組み込まれたロジックによって実行される。以下、図９は、内外フォワーディング先決定ロジックの表である。図１０は、外部フォワーディング先決定ロジックの表である。図１１は、内部ドメインフォワーディング決定ロジックの表である。

【０１０５】フォワード先決定ロジックでは、サービス状態、オペレーション結果、サービスを提供するための相互接続する各ドメインが連結する位置が使用される。図7に示す状態遷移図によって、カスタマから受け付けたサービスの状態が管理され、ドメイン内ルート設計、サービスプロビジョニングの未実行、成功、失敗等の状態がわかる。これらの状態はおのおのサーバで管理するものであるが、別途ネットワークサービス管理装置内に、各装置群の上記サービスの状態を一括管理する装置を設け、おのおののサーバーから、随時書き込み、参照するものであってもよい。状態を遷移させるためのトリガは、図2に示すカスタマケアサーバ、設計サーバ、ポリシーサーバ等のオペレーション実行であるため、サービス状態を参照する事によって処理を要求するサーバが決定される。

【０１０６】また、ドメイン連結内での位置は、ソースドメイン、ミドルドメイン、デスティネーションドメインに三分類される。ソースドメインは、カスタマのソースネットワークと接続されるプロバイダ網を表す。デスティネーションドメインは、カスタマのデスティネーションネットワークと接続されるプロバイダ網を表す。ミドルドメインは、ソースドメインとデスティネーションドメインとの間に位置し、カスタマに対してネットワークリソースを提供するプロバイダ網を表す。例えば、プロバイダ網A、 B、 Cがあり、プロバイダ網Aがカスタマのソースネットワークを収容し、プロバイダ網Cがカスタマのデスティネーションネットワークを収容する場合、プロバイダ網Bがミドルドメインとなる。これらの情報は、ネットワークサービス管理装置内で、認識管理されている。

【０１０７】また、オペレーション結果には、Ｕｎｄｅｆｉｅｎｄ、ＯＫ、ＮＧがある。Ｕｎｄｅｆｉｅｎｄはオペレーション未実行、ＯＫはオペレーション成功、ＮＧはオペレーション失敗を表す。

【０１０８】今、ワークフローサーバ２４Ａによる内外フォワード先決定ロジックにおいて、自ドメインがソースドメインであり、かつ、サービス状態がＡｃｃｅｐｔｅｄであり、かつ、ドメイン間ルートが未設計である場合、外部システムへ処理を移す（ロジックＬ１）。ここで外部システムとは、ネットワークサービス管理装置の内部処理サーバー群外の外部装置を示しているので、プロバイダＡのワークフローサーバ２４Ａから帯域ブローカー２３Ａへ処理が移る。

【０１０９】次に、帯域ブローカー２３Ａでは、処理を

受けて外部フォワード先決定を行う（ステップＣ２）。今、自ドメインがソースドメインであり、かつ、サービス状態がＡｃｃｅｐｔｅｄであり、かつ、ドメイン間ルートが未設計であるので、ドメイン間ルート設計へ処理が移る（ロジックＬ１１）。つまり、外部システム通信手段２３３Ａを介して、マルチドメインサービスブローカー１に処理移管要求のメッセージが送信される。

【０１１０】次に、マルチドメインサービスブローカー１がドメイン間ルート設計を実行する（ステップＣ８）。ドメイン間ルート設計は、ドメイン構成管理手段１３１とサービス管理手段１３２がドメイン構成記憶部１２１、サービス情報記憶部１２２を参照して、カスタマが要求するサービスを満足するドメインの連結を設計する。

【０１１１】ここで、ドメインの連結はカスタマ網のソースネットワークとデスティネーションネットワークを連結するプロバイダのネットワークである。ドメイン間ルート設計後、応答がマルチドメインサービスブローカー１から、プロバイダＡの帯域ブローカー２３Ａに送信される。

【０１１２】次に、プロバイダＡの帯域ブローカー２３Ａは、前記処理を受けて内外フォワード先決定を行う（ステップＣ１）。この時、自ドメインがソースドメインであり、かつ、サービス状態がＡｃｃｅｐｔｅｄであり、かつ、ドメイン間ルートが既設計であるので、内部システムへ処理が移る（ロジックＬ２）。つまり、プロバイダＡのワークフローサーバ２４Ａへ処理が移る。

【０１１３】次に、ワークフローサーバ２４Ａが内部フォワード先決定を行う（ステップＣ９）。今、自ドメインがソースドメインであり、かつ、サービス状態がＡｃｃｅｐｔｅｄであり、かつ、ドメイン間ルートが既設計であり、かつ、自ドメインのオペレーション結果がＵｎｄｅｆｉｎｅｄであるので、ドメイン内ルート設計へ処理が移る（ロジックＬ３１）。つまり、設計サーバ２７が要求されり通信品質を満足するドメイン内部のルートを設計する（ステップＣ１１）。

【０１１４】設計サーバ２７が実行したドメイン内ルート設計の結果は、リソース記憶部２２４とポリシー記憶部２２５に書き込まれる。リソース記憶部２２４には、設計によって新規に割り当てられたネットワークリソース情報を更新する。例えば、１０Ｍｂｐｓの帯域を有するリンクにおいて、１．５Ｍｂｐｓが使用済みであり、新規に１．５Ｍｂｐｓの帯域を割り当てたとき、３．０Ｍｂｐｓのリソースが割り当て済みとなる。ポリシー記憶部２２５には、ネットワーク内の通信装置３に設定するためのコンフィグレーションデータをポリシーとして書き込む。

【０１１５】次に、プロバイダＡのワークフローサーバ２４Ａがドメインの内外フォワード先決定を行う（ステップＣ１）。今、ソースドメインから自ドメインのサービス状態がＩｎｔｒａ　ｄｏｍａｉｎ　Ａｌｌｏｃａｔｅｄであり、かつ、下流ドメインからデスティネーションドメインまでのサービス状態がＵｎｄｅｆｉｎｅｄであるので、外部システムへ処理が移る（ロジックＬ３）。つまり、帯域ブローカー２３Ａへ処理が移る。

【０１１６】次に、帯域ブローカー２３Ａが外部フォワード先決定を行う（ステップＣ２）。今、自ドメインがデスティネーションドメインでなく、かつ、ソースドメインから自ドメインまでのサービス状態がＩｎｔｒａ　ｄｏｍａｉｎ　Ａｌｌｏｃａｔｅｄであり、かつ、下流ドメインからデスティネーションドメインまでのサービス状態がＵｎｄｅｆｉｎｅｄであるので、アドミッションコントロールデシジョンへ処理が移る（ロジックＬ２２、ステップＣ５）。

【０１１７】本実施例の場合、プロバイダＡの運用管理網とプロバイダＢの運用管理網の連結が、カスタマへのサービスへと決定されているので、プロバイダＡのサービスレベル合意管理手段２３１Ａは、サービスレベル合意記憶部２２１Ａを参照して、カスタマの要求するサービス情報が、プロバイダＡとプロバイダＢとの間で合意したサービスに収容できるか否かをチェックする。収容できない場合、入出力装置２１Ａにエラーを表示して処理を終了する。収容できる場合、外部システム通信手段２３３Ａを介して、プロバイダＢの帯域ブローカー２３Ｂ（帯域ブローカーＢ）へサービスプロビジョニング要求を送信する（ステップＣ６）。

【０１１８】帯域ブローカー２３Ｂがサービスプロビジョニング要求を受信すると（ステップＣ７）、内外フォワード決定ロジックを実行する（ステップＣ１）。今、自ドメインがソースドメインでなく、自ドメインのサービス状態がＡｃｃｅｐｔｅｄであり、かつ、オペレーション結果がＵｎｄｅｆｉｎｅｄであるので、内部システムへ処理が移る（ロジックＬ４）。つまり、ワークフローサーバ２４Ｂへ処理が移る。

【０１１９】次に、ワークフローサーバ２４Ｂが、内部フォワード決定ロジックを実行する（ステップＣ９）。今、自ドメインがソースドメインであり、かつ、サービス状態がＡｃｃｅｐｔｅｄであり、かつ、ドメイン間ルートが既設計であり、かつ、自ドメインのオペレーション結果がＵｎｄｅｆｉｎｅｄであるので、ドメイン内ルート設計へ処理が移る（ロジックＣ１）。

【０１２０】次に、設計サーバ２７Ｂが要求された通信品質を満足するドメイン内部のルートを設計し（ステップＣ１１）、ワークフローサーバ２４Ｂへ処理を移管する。

【０１２１】次に、ワークフローサーバ２４Ｂが、内外フォワード決定ロジックを実行する（ステップＣ１）。

【０１２２】今、自ドメインがソースドメインでなく、かつ、すべてのドメインのサービス状態がＩｎｔｒａ　ｄｏｍａｉｎ　Ａｌｌｏｃａｔｅｄであるので、外部シ

ステムへ処理が移る（ロジックＬ５）。つまり、帯域ブローカー２３Ｂへ処理が移管される。

【０１２３】次に、帯域ブローカー２３Ｂが、外部フォワード先決定ロジックを実行する（ステップＣ２）。帯域ブローカー２３Ｂ内のドメインルート管理手段２３２Ｂが、ドメイン構成記憶部２２２Ｂから該カスタマに提供するサービスを実現するためのドメイン連結情報を取得する。本実施例の場合、プロバイダＡの運用管理網とプロバイダＢの運用管理網の連結が登録されているので、ネットワークサービス管理装置群２Ａ、つまり、帯域ブローカー２３Ａに対してサービスプロビジョニング応答を送信する（ステップＣ３）。

【０１２４】帯域ブローカー２３Ａが外部システム通信手段を介して帯域ブローカー２３Ｂからサービスプロビジョニング応答を受信すると（ステップＣ４）、内外フォワード先決定のロジックを実行する（ステップＣ１）。

【０１２５】本実施例の場合、自ドメインがソースドメインであり、かつ、すべてのドメインのサービス状態がＩｎｔｒａ ｄｏｍａｉｎ Ａｌｌｏｃａｔｅｄであるので内部システムへ処理が移管される（ロジックＬ６）。つまり、帯域ブローカー２３Ａの内部システム通信手段を介して、ワークフローサーバ２４Ａに処理が移管される。

【０１２６】次に、ワークフローサーバ２４Ａがネットワークサービス管理装置群２Ａの中での内部フォワード先を決定する（ステップＣ９）。今、自ドメインがソースドメインであり、かつ、すべてのドメインのサービス状態がＩｎｔｒａ ｄｏｍａｉｎ Ａｌｌｏｃａｔｅｄであるので、次の処理はプロビジョニングとなる（ロジックＬ３２）。つまり、ポリシーサーバ２６Ａに処理が移管される。このとき、対象となるサービスＩＤがワークフローサーバ２４Ａからポリシーサーバ２６Ａへ渡される。

【０１２７】ポリシーサーバ２６Ａはサービスｉｄをキーにして、該サービスを提供するための通信装置へのコンフィグレーションデータをポリシー記憶部２２５Ａから読み出す。但し、本実施例の場合、ポリシーサーバ２６Ａがプロビジョニングを行う領域は、プロバイダＡの運用管理網である。

【０１２８】次に、読み出したポリシーデータを通信装置固有のコンフィグレーションデータに変換して、プロビジョニングを実行する（ステップＣ１２）。一般に、通信装置３への設定命令、データは通信装置のメーカーによって異なるが、ポリシーデータは各通信装置とは非依存のコンフィグレーションデータである。

【０１２９】従って、ポリシーサーバは、ポリシーデータを各通信装置に対応した設定命令やデータに変換してプロビジョニングを実行する。プロビジョニングが成功すると、自ドメインのサービス状態をＩｎｔｒａ ｄｏｍａｉｎ ＡｌｌｏｃａｔｅｄからＰｒｏｖｉｓｉｏｎｅｄに変更し、サービス記憶部２２６に格納する。また、自ドメインのプロビジョニングオペレーションの結果をＯＫとして管理する。

【０１３０】ポリシーサーバ２６Ａがプロビジョニングを実行すると、ワークフローサーバ２４Ａへ処理が移管され、内外フォワード先決定を実行する（ステップＣ１）。本実施例の場合、ソースドメインから自ドメインのサービス状態がＰｒｏｖｉｓｉｏｎｅｄであり、かつ、下流ドメインからデスティネーションドメインまでのサービス状態がＩｎｔｒａ ｄｏｍａｉｎ Ａｌｌｏｃａｔｅｄであり、かつ下流ドメインのオペレーション結果がＵｎｄｅｆｉｎｅｄであるので、外部システムへ処理が移管される（ロジックＬ７）。つまり、ワークフローサーバ２４Ａから帯域ブローカー２３Ａへ処理が移管される。

【０１３１】次に、帯域ブローカー２３Ａは、ドメインの外部フォワーディング先決定ロジックを実行する（ステップＣ２）。本実施例の場合、自ドメインがソースドメインでなく、かつ、すべてのドメインでのサービス状態がＩｎｔｒａ ｄｏｍａｉｎ Ａｌｌｏｃａｔｅｄであるので、次の処理はサービスプロビジョニング要求送信となる（ロジックＬ２３）。

【０１３２】帯域ブローカー２３Ａは、ドメイン構成記憶部２２２Ａから該サービスを提供するために経由するドメインの連結情報を取得する。本実施例の場合、プロバイダＡの運用管理網とプロバイダＢの運用管理網の連結となるので、帯域ブローカー２３Ａは帯域ブローカー２３Ｂに対して処理を移管するためのサービスプロビジョニングの要求メッセージを送信する（ステップＣ６）。

【０１３３】帯域ブローカー２３Ｂがサービスプロビジョニングの要求メッセージを受信すると（ステップＣ７）、メッセージが文法的に誤りでないか否かをチェックする。

【０１３４】誤りでない場合、内外フォワード先決定のロジックを実行する（ステップＣ１）。本実施例の場合、ソースドメインから上流ドメインのサービス状態がＰｒｏｖｉｓｉｏｎｅｄであり、かつ、自ドメインからデスティネーションドメインまでのサービス状態がＩｎｔｒａ Ｄｏｍａｉｎ Ａｌｌｏｃａｔｅｄであり、かつ、自ドメインのプロビジョニングのオペレーション結果がＵｎｄｅｆｉｎｅｄであるので、内部システムへ処理が移管される（ロジックＬ８）。つまり、内部システム通信手段２３５を介してワークフローサーバ２４Ｂへ処理が移管される。

【０１３５】次に、ワークフローサーバ２４Ｂは、ネットワークサービス管理装置群Ｂの内部フォワード先決定ロジックを実行する（ステップＣ９）。

【０１３６】本実施例の場合、ソースドメインから上流

ドメインのサービス状態がＰｒｏｖｉｓｉｏｎｅｄであり、かつ、自ドメインからデスティネーションドメインまでのサービス状態がＩｎｔｒａ　ｄｏｍａｉｎ　Ａｌｌｏｃａｔｅｄであり、かつ、自ドメインのオペレーション結果がＵｎｄｅｆｉｎｅｄであるので、次の処理はプロビジョニングとなる（ロジックＬ３３）。つまり、ポリシーサーバ２６Ｂへ処理が移管される。このとき、プロビジョニングを行う対象であるサービスＩＤをポリシーサーバ２６Ｂに渡す。

【０１３７】ポリシーサーバ２６Ｂは、サービスＩＤをキーにして該サービスのポリシーデータをポリシー記憶部２２５Ｂから読み出す。次に、プロバイダＢの運用管理網内で、サービスに関係する通信装置３に対してプロビジョニングを実行し、その結果としてサービス状態を更新する。プロビジョニングに成功した場合、サービス状態をＰｒｏｖｉｓｉｏｎｅｄに変更して、ワークフローサーバ２４Ｂに処理を移管する。

【０１３８】次に、プロバイダＢのワークフローサーバ２４Ｂは、内外フォワード先決定ロジックを実行する（ステップＣ１）。本実施例の場合、マルチドメイン、かつ、自ドメインがソースドメインでなく、かつ、すべてのドメインのサービス状態がＰｒｏｖｉｓｉｏｎｅｄであるので、外部システムへ処理が移管される（ロジックＬ９）。つまり、ワークフローサーバ２４Ｂから帯域ブローカーＢへ処理が移管される。

【０１３９】帯域ブローカー２３Ｂは、ワークフローサーバ２４Ｂからのメッセージを受信すると、外部フォワード先決定ロジックを実行する（ステップＣ２）。本実施例の場合、自ドメインがソースドメインでなく、かつ、すべてのドメインのサービス状態がＰｒｏｖｉｓｉｏｎｅｄであるので、次の処理はサービスプロビジョニング応答送信となる（ロジックＬ２５）。

【０１４０】帯域ブローカー２３Ｂは、ドメイン構成記憶部２２２Ｂから該サービスを実現するためのドメイン連結情報を取得する。本実施例の場合、プロバイダＢの運用管理網の上流ドメインはプロバイダＡであるので、帯域ブローカーＢは、外部システム通信手段２３３を介して、帯域ブローカー２３Ａに対してサービスプロビジョニング応答メッセージを送信する（ステップＣ３）。

【０１４１】帯域ブローカー２３Ａが帯域ブローカー２３Ｂからサービスプロビジョニング応答メッセージを受信すると（ステップＣ４）、内外フォワード先決定ロジックを実行する（ステップＣ１）。本実施例の場合、マルチドメイン、かつ、自ドメインがソースドメインであり、かつ、すべてのドメインのサービス状態がＰｒｏｖｉｓｉｏｎｅｄであるので、内部システムへ処理が移管される（ロジックＬ１０）。つまり、帯域ブローカー２３Ａからワークフローサーバ２４Ａへ処理が移管される。

【０１４２】次に、ワークフローサーバ２４Ａは内部ドメインフォワーディングロジックを実行する（ステップＣ９）。本実施例の場合、自ドメインがソースドメインであり、かつ、すべてのドメインのサービス状態がＰｒｏｖｉｓｉｏｎｅｄであるので、処理を終了する　（ロジックＬ３４）。

【０１４３】以上のように、プロバイダＡのネットワークサービス管理装置群２Ａとプロバイダ Ｂのネットワークサービス管理装置群２Ｂが、サービス登録段階、サービス合意段階、サービスプロビジョニング段階を連携して実行することによって、複数のドメインを介した通信サービスが提供される。

【０１４４】

【発明の効果】本発明の第一の効果は、異なるプロバイダによって運用管理される複数のドメインをまたがる品質保証型通信サービスを提供できる点である。その理由は、各ドメイン内において、設計サーバが要求された品質を満たす通信ルートを計算するだけでなく、帯域ブローカー間の要求と応答のメッセージ交換により、複数のドメイン内での通信ルートが計算されるからである。さらに、ドメイン間の通信品質は、帯域ブローカーがドメイン間の残余リソースを管理することによって保証されるからである。

【０１４５】第二の効果は、カスタマケアサーバ、ポリシーサーバ、設計サーバ、ネットワーク管理装置、ワークフローサーバのシステムメンテナンスやバージョンアップが容易である点である。その理由は、異なるプロバイダとのインタフェース部分を帯域ブローカーのみが有するとともにより、上記のサーバ群の変更が、帯域ブローカーまで波及しにくいからである。

【０１４６】第三の効果は、カスタマケアサーバ、ポリシーサーバ、設計サーバ、ネットワーク管理装置、ワークフローサーバのシステムを他のプロバイダから隠蔽できる点である。その理由は、異なるプロバイダとのインタフェース部分を帯域ブローカーのみが有するとともにより、外部プロバイダから見える処理は、帯域ブローカーが提供するインタフェースのみだからである。

【０１４７】第四の効果は、カスタマ網のソースネットワークからデスティネーションネットワークまでのドメイン間ルートを短時間で算出でき、また、各々のプロバイダが管理する必要がない点である。理由は、マルチドメインサービスブローカーが、提携する全てのドメインのサービス情報を管理することにより、要求されたソースネットワークからデスティネーションネットワークまでを連結するドメイン群を出力できるからである。

【図面の簡単な説明】

【図１】マルチドメインネットワークの構成図である。

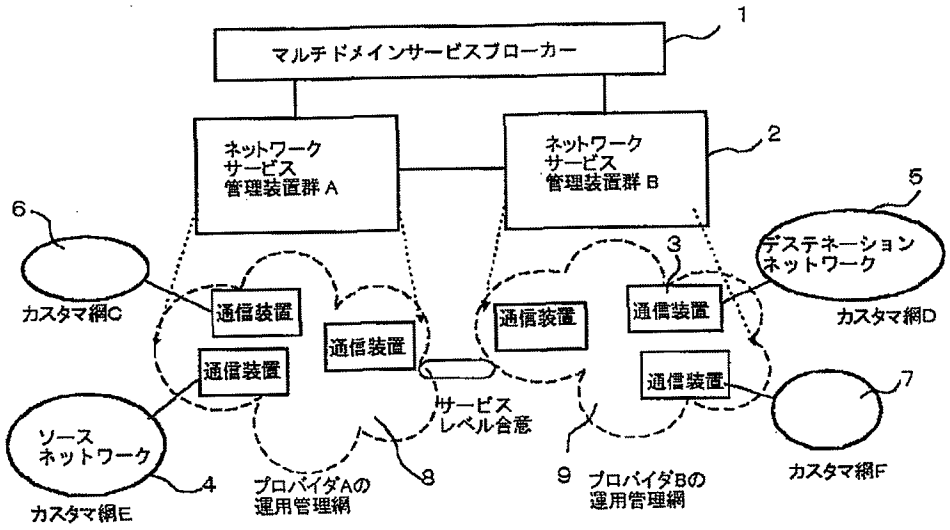
【図２】ネットワークサービス管理装置の機能ブロック図である。

【図３】マルチドメインサービスブローカーの機能ブロック図である。

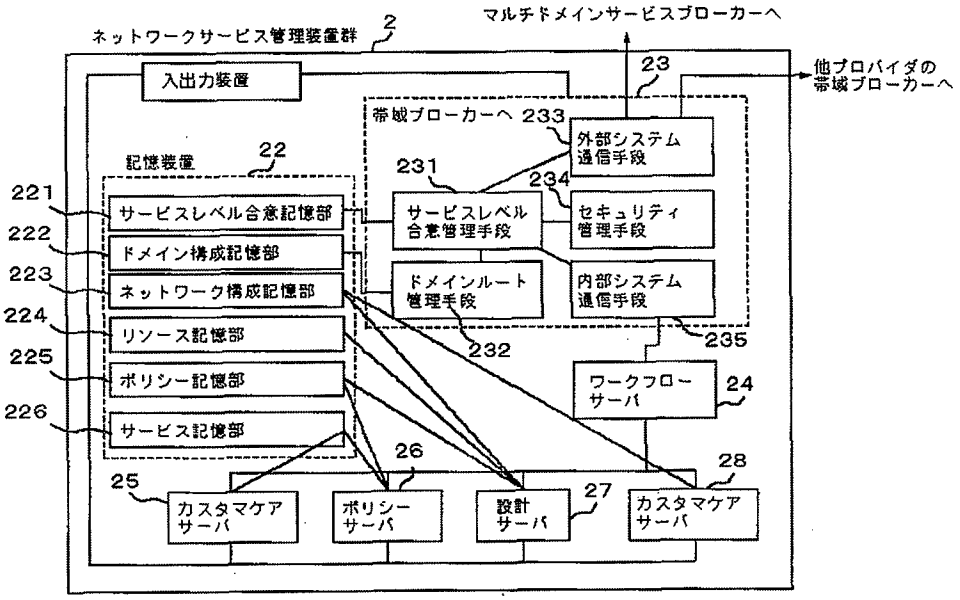
25　　26

【図４】本発明のサービス登録段階の手順を示すフローチャートである。
【図５】本発明のサービス合意段階の動作を示すフローチャートである。
【図６】本発明のサービスプロビジョニング段階の動作を示すフローチャートである。
【図７】本発明のサービスの状態遷移図である。
【図８】サービス状態遷移図の状態表記の説明である。
【図９】内外フォワーディング先決定ロジックの表である。
【図１０】外部フォワーディング先決定ロジックの表である。
【図１１】内部ドメインフォワーディング決定ロジックの表である。
【符号の説明】
１　マルチドメインサービスブローカー
２　ネットワークサービス管理装置群
３　通信装置
４　カスタマ網Ｅ（ソースネットワーク）
５　カスタマ網Ｄ（デステネーションネットワーク）
１１　入出力装置
１２　記憶装置
１３　データ処理装置
２１　入出力装置
２２　記憶装置
２３　帯域ブローカー
２４　ワークフローサーバ
２５　カスタマケアサーバ
２６　ポリシーサーバ
２７　設計サーバ
２８　ネットワーク管理装置
１２１　ドメイン構成記憶部
１２２　サービス記憶部
１３１　ドメイン構成管理手段
１３２　サービス管理手段
１３３　セキュリティ管理手段
１３４　外部システム管理手段
２２１　サービスレベル合意記憶部
２２２　ドメイン構成記憶部
２２３　ネットワーク構成記憶部
２２４　リソース記憶部
２２５　ポリシー記憶部
２２６　サービス記憶部
２３１　サービスレベル合意管理手段
２３２　ドメインルート管理手段
２３４　セキュリティ管理手段
２３５　内部システム通信手段

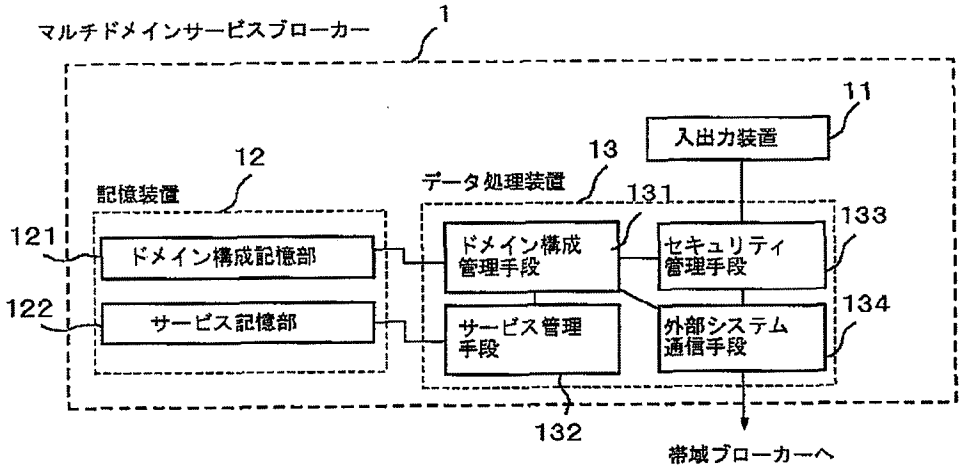
【図１】



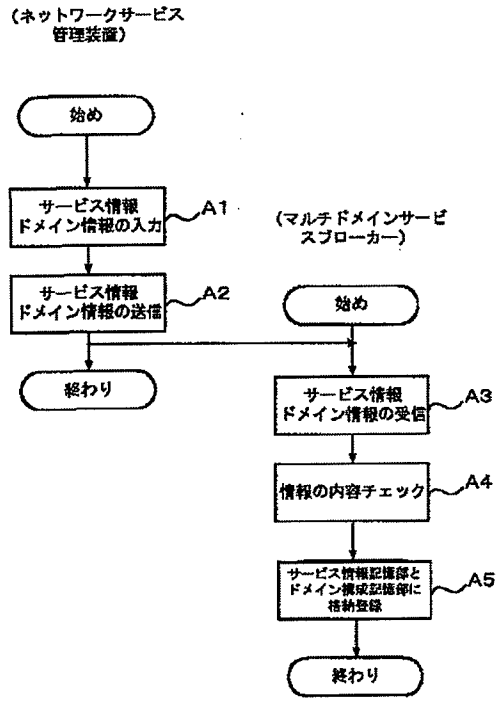
【図２】


ネットワークサービス管理装置群
2
マルチドメインサービスブローカーへ
23
他プロバイダの帯域ブローカーへ
入出力装置
帯域ブローカーへ 233
外部システム通信手段
記憶装置
22
231
234
221
サービスレベル合意記憶部
サービスレベル合意管理手段
セキュリティ管理手段
222
ドメイン構成記憶部
223
ネットワーク構成記憶部
ドメインルート管理手段
内部システム通信手段
224
リソース記憶部
232
235
225
ポリシー記憶部
ワークフローサーバ
24
226
サービス記憶部
26
28
25
27
カスタマケアサーバ
ポリシーサーバ
設計サーバ
カスタマケアサーバ

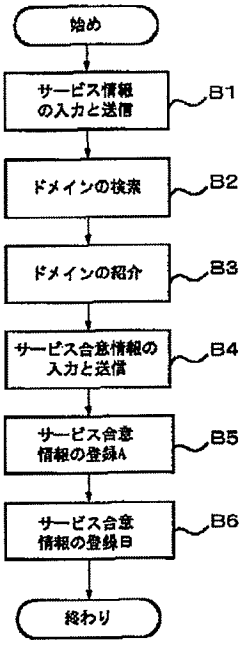
【図３】


マルチドメインサービスブローカー
1
11
入出力装置
12
13
記憶装置
データ処理装置
131
133
121
ドメイン構成記憶部
ドメイン構成管理手段
セキュリティ管理手段
122
サービス記憶部
サービス管理手段
外部システム通信手段
134
132
帯域ブローカーへ

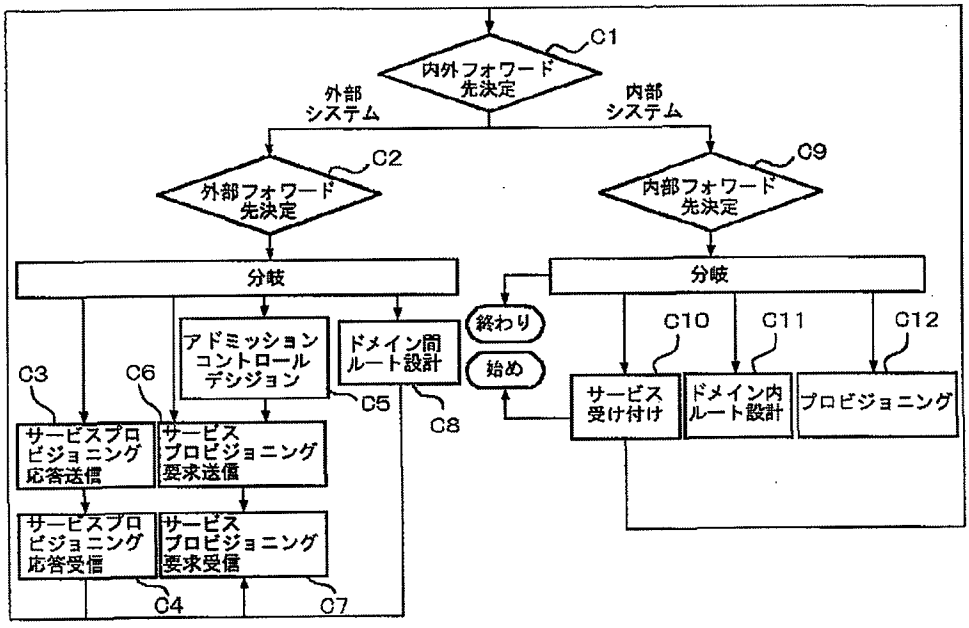
【図４】


(ネットワークサービス管理装置)
始め
サービス情報ドメイン情報の入力
A1
サービス情報ドメイン情報の送信
A2
終わり
(マルチドメインサービスブローカー)
始め
サービス情報ドメイン情報の受信
A3
情報の内容チェック
A4
サービス情報記憶部とドメイン構成記憶部に格納登録
A5
終わり

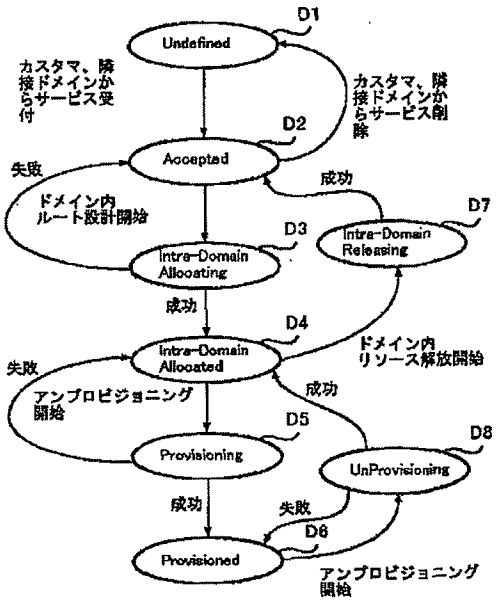
【図５】


始め
サービス情報の入力と送信
B1
ドメインの検索
B2
ドメインの紹介
B3
サービス合意情報の入力と送信
B4
サービス合意情報の登録A
B5
サービス合意情報の登録B
B6
終わり

【図６】


C1
内外フォワード先決定
外部システム
内部システム
C2
外部フォワード先決定
C9
内部フォワード先決定
分岐
分岐
アドミッションコントロールデシジョン
ドメイン間ルート設計
終わり
始め
C3
C6
C5
C8
C10
C11
C12
サービスプロビジョニング応答送信
サービスプロビジョニング要求送信
サービス受け付け
ドメイン内ルート設計
プロビジョニング
サービスプロビジョニング応答受信
サービスプロビジョニング要求受信
C4
C7

【図７】



【図８】

サービス状態	説明
Undefined	サービス受け付け前の状態
Accepted	サービスを受け付けた状態
Intra domain Allocating	ドメイン内ルート設計中の状態
Intra domain Allocated	ドメイン内ルート設計成功後の状態
Intra domain Releasing	ドメイン内ルート解放中の状態
Provisionng	ポリシーのプロビジョニング中の状態
Provisioned	ポリシーのプロビジョニング成功後の状態
Unprovisioning	ポリシーのアンプロビジョニング中の状態

【図９】

内外フォワード先決定ロジック

(ロジックＬ１)自ドメインがソースドメインであり、かつ、サービス状態がAccepted であり、かつ、ドメイン間ルートが未設計のとき、外部システムへ。

(ロジックＬ２)自ドメインがソースドメインであり、かつ、サービス状態がAccepted であり、かつ、ドメイン間ルートが既設計のとき、内部システムへ。

(ロジックＬ３)ソースドメインから自ドメインのサービス状態が Intra domain Allocated であり、かつ、下流ドメインからデスティネーションドメインまでのサービス状態がUndefined のとき、外部システムへ。

(ロジックＬ４)自ドメインがソースドメインでなく、自ドメインのサービス状態がAccepted であり、かつ、オペレーション結果がUndefined のとき、内部システムへ。

(ロジックＬ５)自ドメインがソースドメインでなく、かつ、すべてのドメインのサービス状態がIntra domain Allocated のとき、外部システムへ。

(ロジックＬ６)自ドメインがソースドメインであり、かつ、すべてのドメインのサービス状態がIntra domain Allocated のとき、内部システムへ。

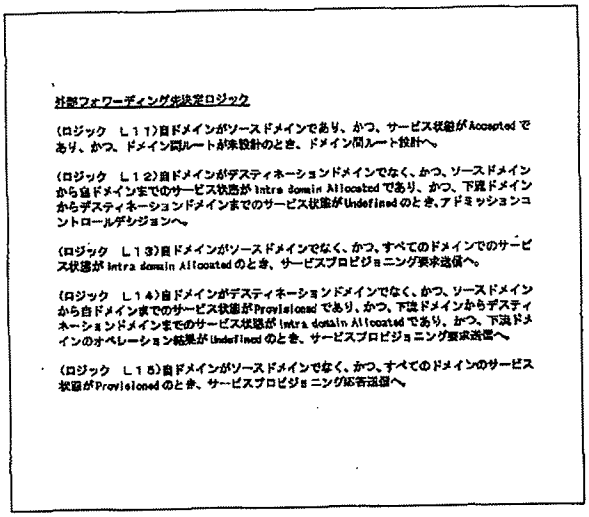
(ロジックＬ７)ソースドメインから自ドメインのサービス状態がProvisioned であり、かつ下流ドメインからデスティネーションドメインまでのサービス状態が Intra domain Allocated であり、かつ下流ドメインのオペレーション結果がUndefined のとき、外部システムへ。

(ロジックＬ８)ソースドメインから上流ドメインのサービス状態がProvisioned であり、かつ、自ドメインからデスティネーションドメインまでのサービス状態が Intra domain Allocated であり、かつ、自ドメインのオペレーション結果がUndefined のとき、内部システムへ。

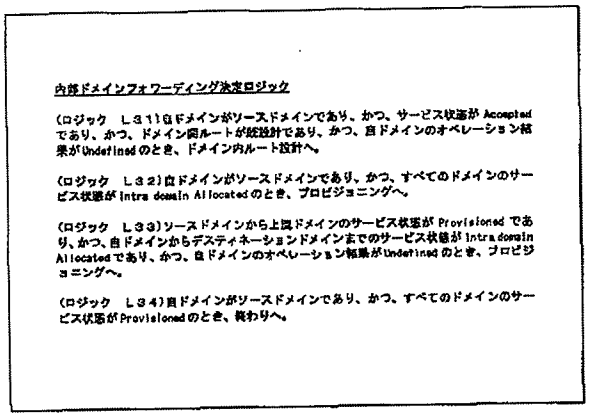
(ロジックＬ９)マルチドメイン、かつ、自ドメインがソースドメインでなく、かつ、すべてのドメインのサービス状態がProvisioned のとき、外部システムへ。

(ロジックＬ１０)マルチドメイン、かつ、自ドメインがソースドメインであり、かつ、すべてのドメインのサービス状態がProvisioned のとき、内部システムへ。

【図１０】


外部フォワーディング先決定ロジック
(ロジック　Ｌ１１)自ドメインがソースドメインであり、かつ、サービス状態がAccepted であり、かつ、ドメイン間ルートが未設計のとき、ドメイン間ルート設計へ。
(ロジック　Ｌ１２)自ドメインがデスティネーションドメインでなく、かつ、ソースドメインから自ドメインまでのサービス状態がIntra domain Allocatedであり、かつ、下流ドメインからデスティネーションドメインまでのサービス状態がUndefinedのとき、アドミッションコントロールデシジョンへ。
(ロジック　Ｌ１３)自ドメインがソースドメインでなく、かつ、すべてのドメインでのサービス状態がIntra domain Allocatedのとき、サービスプロビジョニング要求送信へ。
(ロジック　Ｌ１４)自ドメインがデスティネーションドメインでなく、かつ、ソースドメインから自ドメインまでのサービス状態がProvisionedであり、かつ、下流ドメインからデスティネーションドメインまでのサービス状態がIntra domain Allocatedであり、かつ、下流ドメインのオペレーション結果がUndefinedのとき、サービスプロビジョニング要求送信へ。
(ロジック　Ｌ１５)自ドメインがソースドメインでなく、かつ、すべてのドメインのサービス状態がProvisionedのとき、サービスプロビジョニングOK応答送信へ。

【図１１】


内部ドメインフォワーディング決定ロジック
(ロジック　Ｌ３１)自ドメインがソースドメインであり、かつ、サービス状態がAcceptedであり、かつ、ドメイン間ルートが設計であり、かつ、自ドメインのオペレーション結果がUndefinedのとき、ドメイン内ルート設計へ。
(ロジック　Ｌ３２)自ドメインがソースドメインであり、かつ、すべてのドメインのサービス状態がIntra domain Allocatedのとき、プロビジョニングへ。
(ロジック　Ｌ３３)ソースドメインから上流ドメインのサービス状態がProvisionedであり、かつ、自ドメインからデスティネーションドメインまでのサービス状態がIntra domain Allocatedであり、かつ、自ドメインのオペレーション結果がUndefinedのとき、プロビジョニングへ。
(ロジック　Ｌ３４)自ドメインがソースドメインであり、かつ、すべてのドメインのサービス状態がProvisionedのとき、終わりへ。

(Document 2)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－92059
（P2000－92059A）
(43)公開日　平成12年３月31日(2000.3.31)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/24		Ｈ０４Ｌ　11/08		
12/26		Ｈ０４Ｍ　3/00	Ｄ	
29/10		Ｈ０４Ｌ　13/00	３０９Ｃ	
Ｈ０４Ｍ　3/00				

審査請求　未請求　請求項の数７　ＯＬ　（全５頁）

(21)出願番号　特願平11－240181

(22)出願日　平成11年８月26日(1999.8.26)

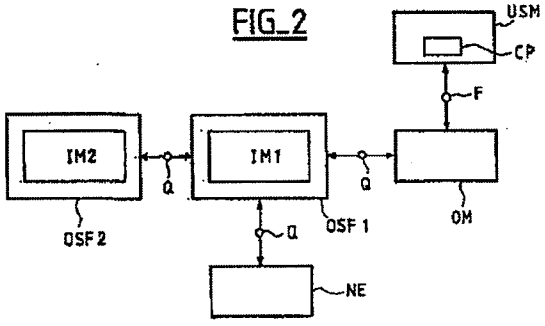
(31)優先権主張番号　９８１０７５９
(32)優先日　平成10年８月27日(1998.8.27)
(33)優先権主張国　フランス（ＦＲ）

(71)出願人　391030332
アルカテル
フランス国、75008　パリ、リュ・ラ・ボエテイ　54
(72)発明者　ロラン・キヤレ
フランス国、78960・ボワザン・ル・プルトヌー、リユ・パン・ゴツグ・26
(74)代理人　100062007
弁理士　川口　義雄　（外２名）

(54)【発明の名称】　電気通信ネットワーク管理システム

(57)【要約】
【課題】　オペレータインターフェースをｑインターフェースに直接基づくものとすることから生じる様々な欠点を解消する。
【解決手段】　本発明による電気通信ネットワーク管理システムは、１つまたは複数のネットワーク情報管理モジュール（ＩＭ１、ＩＭ２）と、１つまたは複数のユーザサービスモジュール（ＵＳＭ）とを含む。本発明によれば、ユーザサービス管理モジュール（ＵＳＭ）のための１つまたは複数のユーザプレゼンテーション層（ＣＰ）をサポートするのに適したインターフェース（ｆ）を含むソフトウェアアーキテクチャを管理システムに搭載することが可能となる。

FIG_2



1

【特許請求の範囲】

【請求項１】　１つまたは複数のネットワーク情報管理モジュール（ＩＭ１、ＩＭ２）と、１つまたは複数のユーザサービスモジュール（ＵＳＭ）とを含む電気通信ネットワーク管理システムであって、システムがユーザサービス管理モジュール（ＵＳＭ）のための１つまたは複数のユーザプレゼンテーション層（ＣＰ）をサポートするのに適したインターフェース（ｆ）を含むソフトウェアアーキテクチャを含むこと、およびソフトウェアアーキテクチャがユーザプレゼンテーション層をサポートするインターフェース（ｆ）と情報管理モジュール（ＯＳＦ）との間に仲介層（ＯＭ）を含むことを特徴とする電気通信ネットワーク管理システム。

【請求項２】　仲介層（ＯＭ）が、ＧＤＭＯ／ＡＳＮ．１言語に基づく情報表現をサポートするプロトコルＣＭＩＰと、ＣＯＲＢＡまたはＩＤＬ言語に基づく情報表現をサポートするＣＯＲＢＡテクノロジーに基づくプロトコルとの間の交換を可能にすることを特徴とする請求項１に記載の電気通信ネットワーク管理システム。

【請求項３】　仲介層（ＯＭ）が、特にＧＤＭＯ言語の継承のためのレイヤの連結や、ＡＳＮ．１タイプから基本タイプへの、またその逆の変形を行うことを特徴とする請求項２に記載の電気通信ネットワーク管理システム。

【請求項４】　インターフェース（ｆ）が、１つまたは複数のタイプのユーザプレゼンテーション層をサポートすることを特徴とする請求項１または２に記載の電気通信ネットワーク管理システム。

【請求項５】　ユーザプレゼンテーション層が、仲介層（ＯＭ）に組み込まれることを特徴とする請求項４に記載の電気通信ネットワーク管理システム。

【請求項６】　ユーザプレゼンテーション層が、ユーザサービス管理モジュール（ＵＳＭ）に組み込まれることを特徴とする請求項５に記載の電気通信ネットワーク管理システム。

【請求項７】　インターフェース（ｆ）がダイレクトグラフィックインターフェース（Ｇ）と、
ユーザがユーザ独自のマクロ命令を記述することを可能にするスクリプト言語（Ｓ）と、
プロトコルＩＩＯＰを介した情報処理ネットワークへのアクセス（ＡＲ）とをサポートすることを特徴とする請求項５または６に記載の電気通信ネットワーク管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は電気通信ネットワーク管理システムに関する。

【０００２】

【従来の技術】電気通信ネットワークは、一般ユーザが通信することを可能にするハードウェア装置とソフトウェア装置のセットによって構成されることを想起されたい。これらの装置としては、特にユーザの電気通信端末がある。なお、この端末は固定端末でも、移動端末でもよい。また、ネットワークへのアクセスシステムや、通信センタ、ネットワーク管理センタがある。

2

【０００３】本発明は、あらゆるタイプの固定または移動電気通信ネットワークに適用される。

【０００４】以下の説明では、とりわけ、「オペレーションシステム」（ＯＳ）という英語によっても知られている電気通信ネットワークの管理センタに関心が寄せられる。これらのセンタは、電気通信ネットワークの事業者が、ネットワークを管理し構成することを可能にする。

【０００５】電気通信ネットワークの管理センタは、５つの機能ブロックＦ、Ａ、Ｃ、Ｐ、Ｓで、すなわち障害管理Ｆ、構成Ｃ、課金に関する情報Ａ、パフォーマンス（品質－伝送速度）ＰおよびセキュリティＳで構成されることを想起されたい。

【０００６】管理センタは、通信ネットワーク自体に対してリアルタイムで働かない。管理センタは、電話呼を確立する必要があるごとにネットワークに入り込む必要はない。つまり、これらのセンタは、ネットワークを監視するために、また遭遇した問題に応じてネットワークを再構成するために、介入する必要がある都度、ネットワークの情報を再組立したり、ネットワークに戻ったりすることを可能にする。

【０００７】管理センタＯＳと電気通信ネットワークの様々な要素との接続は、ＩＴＵによって標準化されている。すべての勧告は、Ｍと名づけられたシリーズとＸと名づけられたシリーズによって定義されている。Ｍシリーズは、実際的な側面に関するものであり、Ｘシリーズは、通信プロトコルやインプリメンテーションに関するものである。

【０００８】主に、ＴＭＮ（電気通信管理ネットワーク：Telecommunication Management Network）と名づけられたコンセプトについて述べているＩＴＵ－Ｔ Ｍ３０１０標準を挙げることができる。このようなＴＭＮの機能上のアーキテクチャは図１に示されている。標準によれば、ＴＭＮは、複数の下記タイプの機能セットを含むことができる。なお、いくつかはオプションである。

【０００９】

・ＯＳＦ（「オペレーションシステム機能」）
・ＷＳＦ（「ワークステーション機能」）
・ＭＦ（「仲介」機能）
・ＱＡＦ（「Ｑアダプタ機能」）
・ＮＥＦ（「ネットワーク要素機能」）

これらのすべての機能について詳述することはしない。なぜならば、いくつかは本発明の枠外にあるからである。

【００１０】管理センタは本来、ＯＳＦ機能とＷＳＦ機

能によって、慣例的に構成されている。ＯＳＦ機能は、厳密に言えば、本来、管理アプリケーションを表している。一方、ＷＳＦ機能は、情報プレゼンテーション機能やユーザとのインターフェース機能を含んでいる。

【００１１】これらのすべての機能セットは、インターフェースを介してセット間で情報を交換することができる。同様に標準によれば、ｆタイプのインターフェースは、ＷＳＦタイプの機能セットをＭＦおよびＯＳＦタイプの機能セットに接続している。ｑ３タイプのインターフェースは、ＯＳＦタイプの機能セットとＯＳＦ、ＭＦ、ＱＡＦおよびＮＦタイプの機能セットとの接続を可能にする。また、ｑｘタイプのインターフェースは、ＭＦ機能セットとＭＦ、ＱＡＦおよびＮＦタイプの機能セットとの接続を可能にする。

【００１２】最後に、ｘ，ｑおよびｍインターフェースは、ＯＳＦ、ＷＳＦおよびＱＡＦセットからのＴＭＮの外部との通信をそれぞれ可能にする。

【００１３】（「ｑリファレンスポイント」とも呼ばれる）ｑインターフェースは、インターフェースモデル化言語によって定義されている。というのは、管理されるネットワークの各要素とは無関係だからである。標準によれば、この記述言語は、ＧＤＭＯ（「Guideline for the Definition of Managed Objects」）言語である。また、データの定義については、ＡＳＮ．１（「Abstract Syntax Notation 1」）言語が用いられている。

【００１４】ｆインターフェースについては、勧告は一般的な規律である。Ｆインターフェースのインプリメンテーション方法を知るための実際の仕様はない。

【００１５】また、現在の技術は、ユーザインターフェース機能（ＷＳＦ）をｑインターフェースに直接基づくものにすることによって成り立っている場合が多い。

【００１６】ところで、ｑインターフェースは、ＷＳＦ機能セットのユーザ（オペレータ）プレゼンテーション層をサポートすることはできない。ｑインターフェースは、管理システム間のダイアログ用である。

【００１７】オペレータインターフェースをｑインターフェースに直接基づくものとすると、次のような欠点を有することとなる。

【００１８】－　ｑインターフェースにおけるオブジェクトの定義とオブジェクトの表現の意味上の隔たりが非常に大きい。したがって、このような機能の開発コストは非常に高い。それゆえに、表現タイプを変えることはきわめてコスト高である。

【００１９】－　ＷＳＦ機能が、システムに全面的に依存するようになる。つまり、ｑインターフェースによって接続できない複数のアプリケーションに共通なＷＳＦ機能を一律にインプリメンテーションすることが容易に可能ではない。

【００２０】ＴＭＮ（「Telecommunication Management Network」）のアーキテクチャの定義標準、ＩＴＵ－Ｔ　Ｍ３０１０標準が、ｆインターフェースであるネットワーク管理システム用のプレゼンテーションインターフェースを定義している。しかし、言われているように、同標準はこのインターフェースの正式な定義についてはあいまいなままである。

【００２１】ＴＭＮアーキテクチャに基づく管理システムは、ｆインターフェースをインプリメンテーションしていない。ユーザインターフェースは、先に述べたように、ＧＤＭＯ／ＡＳＮ．１言語で記述されたインターフェースに直接接続されており、したがって上述の欠点を有している。実際のところ、ｑインターフェースとの所望プレゼンテーション層と同数の、ＯＳＦ機能の働きをもたらす（「User Management System」用）ユーザインターフェースモジュールＵＳＭを開発する必要がある。

【００２２】

【発明が解決しようとする課題】本発明はこれらの欠点を解消することを可能にする。

【００２３】

【課題を解決するための手段】そのため、本発明は、より具体的には、１つまたは複数のネットワーク情報管理モジュールと、１つまたは複数のユーザサービスモジュールとを含む電気通信ネットワーク管理システムを目的とする。このシステムは、それがユーザサービス管理モジュールのための１つまたは複数のユーザプレゼンテーション層をサポートするのに適したインターフェースを含むソフトウェアアーキテクチャを含むこと、またソフトウェアアーキテクチャが、ユーザプレゼンテーション層をサポートしているインターフェースと情報管理モジュールとの間に仲介層を含むことを特徴とする。

【００２４】実際の方法では、電気通信管理ネットワークＴＭＮのｆインターフェースに相当する補足インターフェースが、好ましくは、ユーザサービス管理モジュールＵＳＭ（User Service Manager）に導入される。

【００２５】このインターフェースは、すべてのプレゼンテーションモードに共通なニーズから構築され、そのモデルは、システムによって管理されるエンティティの外部表現に関係している。このｆインターフェースとｑインターフェースとの間には、単一の仲介ソフトウェア層が、設けられるとともに、すべてのユーザプレゼンテーションモジュールによって共有される。

【００２６】本発明のその他の特徴および利点は、添付の図を参照しながら、非限定的な例として示す以下の説明を読むことによって明らかになるであろう。

【００２７】

【発明の実施の形態】図２に示されているように、ネットワーク情報管理モジュールＩＭ１は、リファレンスポイントｑ（すなわち先に定義されたｑインターフェース）を介して、別のネットワーク情報管理モジュールＩＭ２に、あるいはネットワーク装置ＮＥに接続することができる。

【００２８】これらの２つの管理モジュールＩＭ１とＩＭ２は（２つの包括ボックスとして任意に図示されている）２つの機能ＯＳＦ１とＯＳＦ２をそれぞれインプリメンテーションする。

【００２９】また、ユーザインターフェースモジュールＵＳＭも図示されている。

【００３０】本発明によれば、先に言及した理由から、ユーザサービス管理モジュールＵＳＭのための１つまたは複数のユーザプレゼンテーション層ＣＰをサポートするのに適したｆインターフェースを含むソフトウェアアーキテクチャを管理システムに搭載することが提案される。

【００３１】ソフトウェアアーキテクチャは、ユーザプレゼンテーション層ＣＰをサポートしているｆインターフェースと、ユーザサービス管理モジュールＵＳＭに接続されている情報管理モジュールＩＭ１との間に仲介層ＯＭも含む。

【００３２】実際には、ｆインターフェースは、ＴＭＮネットワークの標準化されているｆインターフェースに相当しており、たとえば、ソフトウェアモジュールＵＳＭに導入されることができる。インターフェースは、すべてのプレゼンテーションモードに共通なニーズから構築され、そのモデルは、システムによって管理されるエンティティの外部表現に関係している。

【００３３】このｆインターフェースとｑインターフェースとの間の仲介層ＯＭは、単一であり、すべてのユーザプレゼンテーションモジュール（英語では「PresentationHandler」）によって共有される。

【００３４】図３は本発明によるソフトウェアアーキテクチャをより詳細に示した図である。この図には、図２について先に示された諸要素のいくつかが図示されている。

【００３５】ｑインターフェースからの情報は、たとえば、プロトコルＣＭＩＰ（Common Management Information Protocol）によって運ばれ、電気通信分野のひとつの言語であるＧＤＭＯ／ＡＳＮ．１と呼ばれる言語に従ってモデル化され、仲介層ＯＭによって受け取られる。

【００３６】仲介層のレイヤ１は、このｑインターフェースとのデータ交換の管理を確保する。

【００３７】次に、２、３という参照番号が付されているレイヤは、データ表現モデルＱＭをモデルＦＭに、またデータ表現モデルＦＭをモデルＱＭに切り換えることをそれぞれ可能にする。モデルＦＭとは、データ交換をｆインターフェースを通じて行うために使用されるデータモデルのことである。同様に、モデルＱＭとは、ｑインターフェースのために使用されるデータモデルのことである。

【００３８】レイヤ４については、レイヤ４は、ｆインターフェースのこのデータ表現モデルＦＭを定義する。本発明の実施形態によれば、それはＣＯＲＢＡまたはＣＯＲＢＡ－ＩＤＬ（「Interface Description Language」）テクノロジーに基づく情報表現でもよく、Ｃ＋＋言語でのファンクションコールに基づく情報表現でもよい。

【００３９】したがって、仲介層ＯＭは、データ表現モデルの変形を行うことに加えて、プロトコル変換を行うことができる。

【００４０】たとえば、仲介層ＯＭは、プロトコルＣＭＩＰと、ＩＩＯＰプロトコルまたはＯＭＧ（「Open Management Group」）によって定義されたＣＯＲＢＡタイプのテクノロジーに基づく他のすべてのプロトコルとの間の中継を行うことができる。

【００４１】そのため、仲介層ＯＭは、ＧＤＭＯ言語の継承のためのレイヤの連結や、ＡＳＮ．１タイプから基本タイプへの、またその逆の変形を行う。

【００４２】ｆインターフェースは、複数タイプのユーザプレゼンテーション層をサポートする方が好ましい。

【００４３】一実施形態によれば、ユーザプレゼンテーション層は、仲介層ＯＭに組み込まれることができる。

【００４４】別の実施形態によれば、ユーザプレゼンテーション層は、図３に示されているようにユーザサービス管理モジュールＵＳＭに組み込まれることができる。

【００４５】図示されている実施形態によれば、ｆインターフェースは、下記ユーザプレゼンテーション層をサポートする。

【００４６】－　ダイレクトグラフィックインターフェースＧ－　ユーザ独自のマクロ命令ＦＳ１を、またはファイルに格納されているマクロ命令ＦＳ２を、ユーザがユーザインターフェースＩＵを介して記述することを可能にするスクリプト言語Ｓ－　通信プロトコルＩＩＯＰを介した、様々な情報処理ネットワーク（インターネット、イントラネット）への、またはあらゆるクライアントアプリケーションへのアクセスＡＲまた、Ｆインターフェースは、アジェンダ機能Ａなどのプレゼンテーション層もサポートする。

【００４７】また、仲介層ＯＭに、ロギングモジュールＦ＿Ｌｏｇへのリンクを付加することもできる。その目的はこの層によって行われた変換の記録を可能にすることである。

【００４８】以上説明したソフトウェアアーキテクチャは、ユーザサービスの開放型管理モジュールＵＳＭの提供を可能にする。

【図面の簡単な説明】

【図１】電気通信管理ネットワーク（ＴＭＮ）の機能セットを示した一般図である。

【図２】本発明による管理システムの一般図である。

【図３】本発明によるソフトウェアアーキテクチャの詳細図である。

【符号の説明】

ＣＰ　ユーザプレゼンテーション層

7

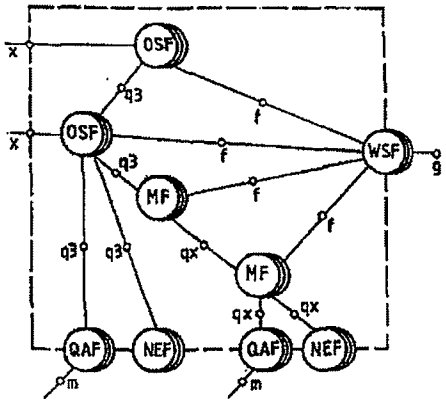
Ｆ　ｆインターフェース
ＩＭ１、ＩＭ２　ネットワーク情報管理モジュール
ＮＥ　ネットワーク装置
ＯＭ　仲介層

8

ＯＳＦ１、ＯＳＦ２　オペレーションシステム機能（情報管理モジュール）
Ｑ　ｑインターフェース
ＵＳＭ　ユーザサービス管理モジュール

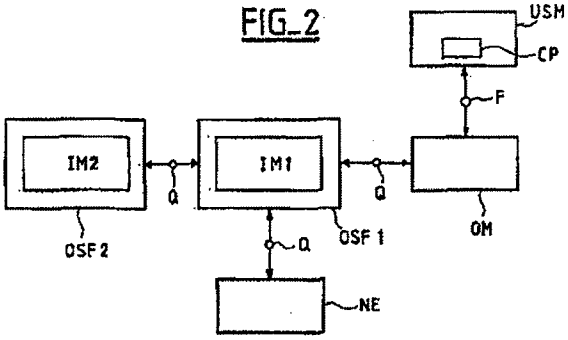
【図１】

FIG_1



【図２】

FIG_2



【図３】

FIG_3